君合研究简讯

JUNHE

2016 年 11 月 15 日

电信与互联网法律热点问题

全国人大常委会正式通过《网络安全法》

全国人民代表大会常务委员会（以下简称“**全国人大常委会**”）在历经长达一年的三次审议后，最终于 2016 年 11 月 7 日通过了《中华人民共和国网络安全法》（以下简称“**《网络安全法》**”）。《网络安全法》是中国第一部关于网络安全的综合性法律，它包含了若干新的法律概念及规定，这些概念及规定将对在中国从事商业运营的公司产生影响。

*君合一直密切关注《网络安全法》制定过程，以及许多与《网络安全法》相关的法律法规。如果您想了解更多背景信息及《网络安全法》的制定过程，请**点击君合往期简讯：***《君合法评 | 网络安全法草案公布征求意见》*、*《君合法评 | 《网络安全法》二审稿的关键修改》*、*《君合法评 | 新国家安全法中涉及信息安全的规定》*、*《君合法评 | 《反恐怖主义法》对电信及互联网行业的影响》*、*《<侵害消费者权益行为处罚办法>关于个人信息保护的规定》。*

以下我们将从出台背景、适用范围及立法目的、主管机关、主要规定、《网络安全法》终稿与一审、二审稿的比较以及潜在实践影响的角度对《网络安全法》进行简要介绍。

一、简介

（一）出台背景

为国家安全整体形势所需要，近年来关于信息和科技安全的立法及司法实践迅速发展。2014 年 4 月，为应对新时期的各种挑战，习近平总书记第一次提出了“总体国家安全观”的概念。此后，全国人大常委会加快了一系列与国家安全相关法律的立法工作，包括《反恐怖主义法》、《国家安全法》以及《网络安全法》。这些立法都涉及有关信息和技术安全的规定。网络安全在中国及全世界都成为对于社会的一项挑战，而《网络安全法》是回应这些挑战的关于网络安全方面的主要立法。同时，由于中国尚未出台一部统一的信息保护法，但个人信息保护问题已成为广泛关注的社会问题，因此《网络安全法》也包含了许多与个人信息保护有关的规定，除对以往散见于各法规的要求的总括性规定，也包括一些新的法律要求。

（二）适用范围及立法目的

《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。“网络”是指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（第七十六条）。《网络安全法》将“网络运营者”广泛地定义为“网络的所有者、管理者和网络服务提供者（第七十六条）”。

《网络安全法》将“维护网络空间主权”规定为基本原则。为实现这一目的，《网络安全法》对网络安全、网络运营安全、网络信息安全、网络安全预警和应急处置系统等各方面问题作出了规定。

（三）网络安全主管机关

根据《网络安全法》，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，即国家互联网信息办公室。此外，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）。

《网络安全法》将于 2017 年 6 月 1 日生效，距其实施还有约半年的过渡期。

二、主要法律规定

（一）加强网络运营者的安全义务

《网络安全法》对网络运营者规定了一系列安全义务，其中包括：

- 遵守网络安全等级保护制度的一系列要求（第二十一条）；
- 核实用户真实身份（部分网络运营者的义务）（第二十四条）；
- 制定网络安全事件应急预案（第二十五条）；以及
- 为侦查机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助（第二十八条）。

此外，网络产品、服务的提供者发现其网络产品、服务存在安全缺陷、漏洞等风险时，应及时告知用户并向有关主管部门报告；应当为其产品、服务持续提供安全维护；不得设置恶意程序；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（第二十二条）。

网络关键设备和网络安全专用产品应当遵守相关国家标准及强制性资格要求，并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，方可销售或者提供（第二十三条）。

值得注意的是，《网络安全法》中许多有关网络运营者的规定首次出现在我国法律中，例如：留存相关的网络日志不少于六个月（第二十一条）；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活动的规制（第二十六条）等。

（二）加强对关键信息基础设施的保护

《网络安全法》在我国法律中首次对关键信息基础设施运营者施加了更严格的安全保护义务，这些义务包括：

- 设置内部专门机构、负责人，进行内部培训，数据备份以及制定网络安全事件应急预案（第三十四条）；
- 原则上，在中华人民共和国境内运营中收集和产生的个人信息和重要数据需存储在境内（第三十七条）；
- 采购网络产品和服务，可能影响国家安全的，应当通过相关政府部门的国家安全审查（第三十五条）；以及
- 对网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关政府部门（第三十八条）。

（三）个人信息保护

《网络安全法》重申了网络运营者对个人信息的保护义务，这些义务散见于现有法律、法规，包括：网络运营者收集、使用个人信息，遵循合法、正当、必要的原则和“知情和同意”的要求（第四十一条）；仅将个人信息用于个人同意的目的（第四十一条）；采取安全保护措施以确保个人信息的安全（第四十二条）；保护个人查阅和更正其个人信息的权利（第四十三条）。此外，《网络安全法》还包含了一些关于个人信息的新规则，例如：数据泄露通知义务（第四十二条）；个人信息的收集、使用需遵守知情和同意原则，但信息经过处理无法识别特定个人且不能复原的除外（第四十二条）；个人在发现被收集、存储的其个人信息有错误的或者个人信息的收集、使用违反双方的约定的时候，有权要求网络运营者进行修改或者删除相关个人信息（第四十三条）。

三、对二审稿的关键修改

相较二审稿，《网络安全法》有如下关键修改：

1、 关键信息基础设施被重新定义为“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域”，以及其他“一旦遭到破坏、丧失功能或者数据泄露，可

能严重危害国家安全、国计民生、公共利益”的信息基础设施。定义中对相关行业及领域的列举曾体现在《网络安全法》一审稿中，但在二审稿中被删除。正式的《网络安全法》将对重要行业和领域的列举重新加入到关键信息基础设施的定义里（第三十一条）。

2、 具有境内存储要求的信息范围由“公民个人信息和重要业务数据”扩大为“个人信息和重要数据（第三十七条）”；受保护的个人信息的范围由“公民个人信息”扩大为“个人信息”；

3、 对未成年人的特别规定：国家支持研究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危害未成年人身心健康的活动（第十三条）；

4、 增加了对境外实体危害关键信息基础设施罚则和制裁的专门规定（第七十五条）；以及

5、 增加了对违法行为的处罚力度。

四、实践影响

《网络安全法》是我国第一部专门针对网络安全问题的法律。2017 年 6 月 1 日《网络安全法》正式实施后，在中国从事互联网及其他涉及网络运营的各行业经营者将需履行更严格和全面的法律义务，并将因违反相关义务受到更重的处罚。作为一部关于网络安全的整体性、综合性法律，《网络安全法》之中对于很多方面作出的规定仍是高屋建瓴的，而在实施和执行的细节方面，仍将依赖于更为具体的规定和主管部门的实施意见出台。可以预见，相关主管机关可能会颁布一系列实施细则以落实《网络安全法》的要求，例如：网络安全等级保护制度；关键信息基础设施的具体范围及保护措施；对未成年人在互联网领域的保护；网络关键设备和网络安全专用产品的强制性安全认证及检测要求；关键信息基础设施采购网络产品和服务时，应通过的国家安全审查等。例如，关于未成年人在互联网领域的保护问题，网信办即已于 2016 年 10 月发布了《未成年人网络保护条例》（草案）向公众征求意见。

现在距离《网络安全法》的正式实施还有大约半年的时间，相关公司可以利用这一过渡期理解《网络安全法》可能对于公司运营的影响。特别是，若公司被纳入到关键信息基础设施运营者的范畴，则《网络安全法》将可能对于其网络安全架构、安全产品采购、数据存储等方面产生实质性的重大影响。公司需要从这些方面综合性的考虑是否需要采取业务和经营的调整，加强其网络安全保护以确保符合《网络安全法》的规定。考虑到《网络安全法》中的相关要求的实施标准并不完全明确，公司在未来需继续关注相关新法规以及主管机关的实施意见，以对法律的适用作更好的理解。

董　潇　合伙人　电话：86 10 8519 1233　邮箱地址：dongx@junhe.com
蔡克蒙　律　师　电话：86 10 8519 1255　邮箱地址：caikm@junhe.com
郭静荷　律　师　电话：86 10 8553 7947　邮箱地址：guojh@junhe.com

JUN HE BULLETIN

JUNHE

Nov 15, 2016

Telecommunication Law

Cyber Security Law Adopted by the NPC Standing Committee

After three deliberations over more than a year's time, the Standing Committee of the National People's Congress ("**NPC Standing Committee**") finally adopted the *Cyber Security Law* ("**CSL**") on November 7, 2016. The CSL is the first omnibus law in China governing cyber security issues and has incorporated a number of new legal concepts and requirements that may impact companies with business operations in China.

JunHe has been closely following the development of the drafts of the CSL, as well as a number of laws and regulations relevant to the CSL. If you are interested in understanding the background and evolution of the CSL drafts, please ***click the following alerts:*** *Draft of Cyber Security Law Released for Public Comments*, *Key Changes in Second Draft Cyber Security Law*, *National Security Law includes Information Security Provisions*, *China Adopted the Counter-Terrorism Law*

Below we will briefly introduce the CLS in terms of the context of its development, the applicable scope and legislative purpose, the major requirements, a brief comparison between the final CSL and the first and second drafts, and the potential practical impact.

1. Introduction

Background

The information and technology security related legislation and practice developed quickly in recent years due to the need for protecting China's national security. In April 2014, in response to various challenges of the new era, President Xi Jinping for the first time raised the "overall concept of national security". Thereafter, a series of legislations relating to national security were put on an accelerated track, including the Counter-terrorism Law, the National Security Law and the Cyber Security Law. These legislations all include provisions relating to information and technology security. Cyber security is currently a challenging matter both in China and around the world, and the CSL, in response to these challenges, represents major legislation with respect to cyber security issues. Meanwhile, as China has not enacted a unified data protection law, the CSL also

incorporates several provisions related to the protection of personal information, which has also emerged as an issue of wide concern. Apart from some general provisions on personal information which were embodied in several existing regulations, the CSL also includes some new requirements on this issue.

Application Scope and Purpose

The CSL applies to the construction, operation, maintenance and use of networks as well as the supervision and administration of cyber security within the territory of the PRC. "Networks" include networks and systems that are composed of computers and other information terminals and the relevant facilities and used for purpose of collecting, storing, transmitting, exchanging and processing information in accordance with certain rules and procedures (Article 76). "Network operators", an important subject of legal obligations under the CSL, is broadly defined as "owners and administrator of networks and network service providers (Article 76)".

The CSL provides for "safeguarding the national cyberspace sovereignty" as a fundamental principle, and, for that purpose, 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.

Responsible Authority

The national cyberspace administration authority, namely the Cyberspace Administration of China ("**CAC**"), is responsible for the coordination of cyber security protection activities and the relevant supervision and administration activities 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 authorities.

Transition Period

The CSL will become effective on June 1, 2017. Therefore, nearly a half year is provided for a transition period before its implementation.

2. Major Legal Requirements

Strengthened Network Operation Security Obligations

The CSL provides various security protection obligations for network operators, including, *inter alia:*

- the compliance with a series of requirements of tiered cyber protection systems (Article 21);
- the verification of users' real identity (an obligation for certain network operators) (Article 24);
- the formulation of cyber security emergency response plans (Article 25); and
- the assistance and support necessary to investigative authorities where necessary for protecting national security and investigating crimes (Article 28).

In addition, network products and service providers shall inform users about and report to

the relevant authorities any known security defects and bugs, and furthermore shall provide constant security maintenance services for their products and services, not install malware with their products, and clearly inform users and obtain their consent if their products or services collect users' information (Article 22).

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 organization or passing the relevant security tests (Article 23).

It is notable that some requirements for network operators, such as retention of user logs for at least six months (Article 21) and regulations on the publication of cyber security information regarding system loopholes, computer viruses, cyber-attacks, cyber invasions, etc. (Article 26), are prescribed for the first time under PRC laws.

Heightened Protection of Critical Information Infrastructure

The CSL, for the first time under PRC law, clearly imposes a series of heighted security obligations for operators of critical information infrastructure ("**CII**"), including:

- internal organization, training, data backup and emergency response requirements (Article 34);
- storage of personal information and other important data must be secured within the PRC territory, in principle (Article 37);
- procurement of network products and services which may affect national security shall pass the security inspection of the relevant authorities (Article 35); and
- conduct annual assessments of cyber security risks and report the result of those assessments and improvement measures to the relevant authority (Article 38).

Protection of Personal Information

The CSL reiterates the obligations of network operators regarding the protection of personal information which appear across existing laws and regulations, including the mandate to observe the principle of lawfulness, necessity and appropriateness in the collection and use of personal information and to observe "the inform and consent requirements" (Article 41), to use personal information only for the purpose agreed upon by the relevant individual (Article 41), to adopt security protection measures for personal information (Article 42), and to protect the individual's right to access and correct personal information (Article 43). In addition, the CSL also incorporates some new rules on personal information protection, including data breach notification requirements (Article 42), and data anonymization as an exception for inform and consent requirements (Article 42), and the individual's right to request the network operators make corrections to or delete their personal information in case the information is wrong or used beyond the agreed purpose (Article 43).

3. Key Differences from the Second Draft

The Final Draft reflects the following key changes from the Second Draft.

- CII is rephrased as information infrastructure in "public communication and information services, energy, traffic and transportation, irrigation, finance, public service, e-government and other key industries and sectors", as well as other information infrastructure, "the damage, malfunction and data leakage of which may seriously endanger national security, national welfare, people's livelihood, and public interest." The enumeration of industries and sectors, which was included in the first drafted of the CLS and removed in the Second Draft, is added back into the definition of CII under the final CSL (Article 31);
- the scope of CII data subject to local storage requirements is expanded from "citizen's personal information and other important business data" to "personal information and important data" (Article 37);
- the protected personal information is expanded from "citizen's personal information" to "personal information";
- a special provision for minors which provides the State supports the research and development of network products and services that are helpful to the healthy development of minors, and imposes punishments upon any person who uses networks to carry out any activity endangering the physical and mental health of minors （Article 13）;
- an additional special provision on punishments and sanctions against overseas entities which endanger domestic CII（Article 75）; and
- higher monetary punishments imposed for violations.

4. Practical Impacts

The CSL is the first law in the PRC specially focused on cyber security matters. When the CSL takes effect on June 1, 2017, internet companies and other industries in China will be subject to a wide array of stricter and more comprehensive obligations and face more severe punishments for potential violations. As an omnibus law on cyber security issues, many provisions of the CSL are still very general and abstract, and the detailed requirements for implementation and enforcement depend on subsequent and more specific implementation regulations as well as the opinion of the relevant authorities. We may expect that the relevant regulatory authorities may promulgate a series implementation regulations to clarify certain requirements under the CSL, such as the regulations on tiered cyber security protection systems, the specific scope and protection measures of CII, the protection of minors on networks, the mandatory security certification and the test requirements for key network devices and special cyber security products, national security review on the network products and services procured by CII operators, etc. For example, as for the protection of minors on the internet, last month the CAC published a draft for public comment of *Regulations on Protection of Minors Online*.

Nearly half a year remains before the formal implementation of the CSL and companies may use this transition period to improve their understanding of the potential impacts of the CSL on their business. In particular, if companies are deemed operators of CII, the CSL may have a significant impact on its network security framework, procurement of security products, and data storage. Companies may consider whether they need to adjust their business and operation practices from these aforementioned aspects and enhance their cyber security protections so as to ensure fully compliance with the CSL. Given the specific implementation of the requirements in the CSL are not entirely clear, companies will also need to closely follow any subsequently released regulations and opinions of the relevant governmental authorities.

Marissa DONG	Partner	Tel: 86 10 8519 1233	Email:dongx@junhe.com
Kemeng CAI	Associate	Tel: 86 10 8519 1255	Email:caikm@junhe.com
Jinghe Guo	Associate	Tel: 86 10 8553 7947	Email:guojh@junhe.com