JUN HE BULLETIN

JUNHE

July 21, 2016

Telecommunication Law

Key Changes in Second Draft Cyber Security Law

The full text of the second draft (the "**Second Draft**") Cyber Security Law (the "**CSL**") was released on July 5, 2016 to solicit public comment until August 5, 2016, after its second deliberation during the 21st session of the 12th NPC Standing Committee. The key differences between the Second Draft and the first draft of CSL released in July 2015 (the "**First Draft**") are briefly summarized as below.

I. Enhanced Obligations of Network Operators

The Second Draft further imposes and specifies certain obligations of network operators, including:

(i) Network operators shall comply with laws and regulations, uphold social and commercial moral standards, perform cyber security protection obligations, accept government and public supervision, and observe social responsibility (Article 9);

(ii) The period for network operators to retain network logs is at least six months (Article 20);

(iii) Network operators providing instant message services are clearly required to verify users' identities (Article 21);

(iv) Network operators shall cooperate with the supervision and inspection of cyberspace administrative authorities and other relevant authorities (Article 47).

II. Revision to the Definition and Protection of Critical Information Infrastructure ("CII")

There are several major changes with respect to the definition and protection of CII. Firstly, the Second Draft removes the definition of CII with specific enumeration and leaves the specific

scope of CII to the implementing regulation of the CSL to be issued by the State Council (Article 29). Secondly, the Second Draft has rephrased the scope of CII data subject to local storage requirements from "citizen's personal information and other important data" in the First Draft, to "personal information and other important business data" (Article 35) in the Second Draft. Thirdly, the Second Draft adds that the State encourages network operators falling outside the statutory scope of CII to join the CII protection system voluntarily (Article 29). Fourthly, the Second Draft stipulates that the information obtained by the cyber administrative and other authorities from the CII protection activities shall only be used for cyber security protection purposes (Article 38).

III. Some Other Changes

The Second Draft also incorporates some other changes. For example, firstly, the Second Draft restricts the release of cyber security information regarding system loopholes, computer viruses, cyber-attacks, cyber invasions and etc. (Article 25). Secondly, the Second Draft provides that application of big data could only be carried out on the basis of data anonymization (Article 41). Thirdly, the State promotes the opening public data sources, and supports the development of cyber security management measures, utilization of new technologies and promotion of overall network security levels (Article 17). Fourthly, the punishments for violation of the CSL are more severe under the Second Draft.

The implications of these changes remain to be evaluated by companies in different industries and areas.

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

君合研究简讯

JUNHE

2016 年 7 月 21 日

电信法律热点问题

《网络安全法》二审稿的关键修改

全国人大常委会公布了经第十二届全国人大常委会第 21 次会议审议的《网络安全法》的二审稿全文（以下简称“**二审稿**”），并于 2016 年 7 月 5 日至 2016 年 8 月 5 日期间向社会公开征求意见。相较 2015 年 7 月公布的《网络安全法》一审稿（以下简称“**一审稿**”），二审稿有以下主要修改。

一、提高了网络运营者的义务

二审稿进一步细化或增加了网络运营者的特定义务，包括：

（1） 网络运营者必须遵守法律、行政法规，遵守社会公德、商业道德，诚实信用，履行网络安全保护义务，接受政府和社会公众的监督，承担社会责任（第 9 条）；

（2） 网络运营者网络日志不少于六个月（第 20 条）；

（3） 提供即时通讯服务的网络运营者被明确要求对用户身份进行验证（第 21 条）；

（4） 网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合（第 47 条）。

二、涉及关键信息基础设施定义和保护措施的修改

与一审稿相比，二审稿对关键信息基础设施的含义和保护措施做了一些关键修改。第一，二审稿删除了对关键信息基础设施列举式的定义，并将关键信息基础设施的具体范围和保护办法留待国务院确定（第 29 条）。第二，二审稿将关键信息基础设施运营者需要在中国境内存储的数据的范围由一审稿中规定的“公民个人信息等重要数据”改为“公民个人信息和重要业务数据”（第 35 条）。第三，二审稿增加了“国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系”的规定（第 29 条）。第四，二审稿规定，国家网信部门和有关部门在关键信息基础设施保护中获取的信息，只能用于维护网络安全的需要，不得用于其他用途（第 38 条）。

三、一些其他的修改

二审稿还进行了一些其他的修改。例如，二审稿对擅自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进行了限制（第 25 条）；对大数据的利用必须建立在数据匿名化的基础上（第 41 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（第 17 条）。此外，二审稿增加了对违法行为的处罚力度。

上述修改对不同行业和领域的企业的影响还需要进一步观察评估。

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