君合研究简讯

JUNHE

2022 年 9 月 23 日

网络安全法律热点问题

网安法修订草案发布

2022 年 9 月 14 日，国家网信办发布《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》（以下简称“**《征求意见稿》**”），向社会公开征求意见，意见反馈截止时间为 2022 年 9 月 29 日。[1]作为中国网络安全及数据保护立法的三驾马车之一，自 2017 年起已施行 5 年之久的《网络安全法》将迎来首次修订。

本次修改主要针对网络运行安全、关键信息基础设施安全保护、网络信息安全以及个人信息保护四方面的法律责任制度。修改内容体现了与《数据安全法》、《个人信息保护法》、《行政处罚法》等新实施的法律之间的衔接协调，也与实践中网络安全领域执法不断加强的趋势相呼应。《征求意见稿》主要修改意见总结如下。

一、完善违反网络运行安全一般规定的法律责任制度

《网络安全法》第二十一条、第二十二条第一款和第二款、第二十三条、第二十四条第一款、第二十五条、第二十六条、第二十八条对网络运营者需遵循的网络运行安全保护义务进行了规定，包括：（1）网络安全等级保护制度；（2）网络产品、服务符合相关国家标准强制性要求的义务及其他安全保护义务；（3）网络关键设备和网络安全专用产品的安全认证合格或者安全检测义务；（4）网络运营者实名认证义务；（5）制定及遵守网络安全事件应急制度的义务；（6）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；（7）为相关政府部门法维护国家安全和侦查犯罪的活动提供技术支持和协助。

《征求意见稿》对违反该等规定的罚则进行了调整，变化主要包括：

1. **对网络运营者违法行为新增行政处罚种类。**新增种类包括通报批评、责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

2. **上调对网络运营者、直接负责的主管人员和其他直接责任人员的罚款额度**。网络运营者发生前述违法行为，拒不改正的，罚款额度由原来的“一万元以上十万元以下罚款”调整为“一百万元以下罚款”；对直接负责的主管人员和其他直接责任人员的罚款金额幅度从五千元以上五万元以下上调为一万元以上十万元以下。

3. **增加情节特别严重情形下的罚则**。情节特别严重的，将对网络运营者处一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

[1] 国家互联网信息办公室发布《关于修改<中华人民共和国网络安全法>的决定（征求意见稿）》，http://www.cac.gov.cn/2022-09/14/c_1664781649609823.htm

4. **对《网络安全法》中原本并未设置相应罚则的条款增加了罚则**，包括《网络安全法》第二十三条以及第二十八条。

5. **在网络运行安全保护方面，《征求意见稿》还对违反《网络安全法》第二十七条的法律责任进行了更新。**《网络安全法》第二十七条规定：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的活动，不得为他人从事该等活动提供技术支持等帮助。《征求意见稿》在原法律责任规定的基础上，增加了针对单位的处罚措施以及对从事前述活动的人员的从业限制措施。

二、修改关键信息基础设施安全保护的法律责任制度

《网络安全法》第三十三条、第三十四条、第三十六条、第三十八条对关键信息基础设施建设的安全要求、关键信息基础设施运营者的安全保护义务、关键信息基础设施采购的安全保密义务以及关键信息基础设施的定期安全检测评估义务进行了规定。《征求意见稿》对违反前述规定的法律责任进行了调整，具体体现在：

1. **对关键信息基础设施运营者违法行为新增行政处罚种类**。增加行政处罚种类，新增种类包括通报批评、责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；

2. **对于拒不改正的情形取消罚款下限**。罚款金额从“十万元以上一百万元以下”调整为“一百万元以下”，取消了对罚款金额下限的设置；

3. **增加情节特别严重情形下的罚则**。具体内容与前述网络运营者违反网络运行安全一般规定的罚则一致。

4. **对违反信息出境义务进行了转致性规定**。《网络安全法》第三十七条要求，关键信息基础设施运营者在中国境内运营中收集和产生的个人信息和重要数据应当在境内存储；因业务需要，确需向境外提供的，应当进行安全评估。对于违反该项义务的法律责任，《征求意见稿》则进行了转致性规定，要求“依照有关法律、行政法规的规定处罚”。具体而言，关键信息基础设施运营者违反前述规定向境外提供重要数据的，依照《数据安全法》第四十六条进行处罚；关键信息基础设施运营者违反前述规定向境外提供个人信息的，依照《个人信息保护法》第六十六条等规定进行处罚。

三、调整网络内容安全法律责任制度

《征求意见稿》对《网络安全法》第四十七条、第四十八条、第四十九条的罚则进行了修改。前述条款对网络运营者需遵循的网络内容安全义务进行了规定，包括及时处置用户发布或传输的违法信息、禁止在发送的电子信息或提供的应用软件中设置恶意程序、建立网络信息安全投诉、举报制度等。《征求意见稿》对前述条款对应罚则的修改主要体现在：

1. 对网络运营者违反网络信息安全保护义务的行为，增加了“通报批评”这一项行政处罚；

2. 对拒不改正或者情节严重的情形，将罚款上限从原来的“五十万元”上调为“一百万元”；

3. 增加情节特别严重情形下的罚则，具体内容与前述网络运营者违反网络运行安全一般规定的罚则一致；

4. 对《网络安全法》第十二条第二款禁止利用网络发布或传输有关违法信息，以及第四十六条禁止设立用于实施违法犯罪活动的网站、通讯群组或者发布涉及实施违法犯罪活动的信息，上调了对相关个人和组织的罚款额度。

四、修改个人信息保护法律责任制度

《征求意见稿》对违反《网络安全法》第二十二条第三款、第四十一条至第四十四条的法律责任制度进行了修改。该等条款涉及对网络运营者在个人信息保护方面的相关要求，包括收集、使用个人信息需遵循合法、正当、必要原则、采取必要措施确保个人信息安全的义务、响应个人关于删除或更正其个人信息要求的义务等。《网络安全法》已对

违反前述条款的法律责任进行了详细规定，鉴于《个人信息保护法》规定了全面的个人信息保护法律责任制度，为与《个人信息保护法》做好衔接，《征求意见稿》则将原有关个人信息保护的法律责任修改为转致性规定。

五、总结

《征求意见稿》未对网络运营者增加新的具体合规义务类型，但从整体上对网络运营者（包括关键信息基础设施运营者）在网络运行安全、网络信息安全以及个人信息保护方面的法律责任进行了更加严格的规定。例如，对网络运营者最高处以上一年度营业额百分之五以下罚款，以及对直接负责的主管人员和其他直接责任人员最高处一百万元罚款以及一定期限内的从业限制，将极大提高网络运营者及管理人员的合规风险及成本。上述修改方向体现了《个人信息保护法》的最新规定及近期实践中执法案例所展示的监管趋势。

我们建议企业持续关注《网络安全法》修订动态，结合《网络安全法》相关要求进行合规自查，确保企业按照《网络安全法》的要求履行相关法定义务。

董　潇　合伙人　电话：86-10 8519 1718　邮箱地址：dongx@junhe.com
郭静荷　律　师　电话：86-10 8553 7947　邮箱地址：guojh@junhe.com
周　佳　律　师　电话：86-21 2208 6119　邮箱地址：zhouj_lark@junhe.com

Cybersecurity Law

Cybersecurity Law Exposure Draft Released

On September 14, 2022, the Cyberspace Administration of China (CAC) issued the Decision of Amending the Cybersecurity Law of the People's Republic of China (Exposure Draft) to solicit public opinion until September 29, 2022. It is one of the three major laws in China's cybersecurity and data protection legislation and will be revised for the first time since 2017. [2]

The revisions mainly focus on legal liability in four areas: the security of network operations, the security protection of critical information infrastructure, network information security and the protection of personal information. They reflect the connection and coordination between the Data Security Law, the Personal Information Protection Law, the Administrative Penalties Law, and other newly implemented laws. The Exposure Draft aligns with the trend for continuous law enforcement in the field of cybersecurity. The main revision of opinions in the Exposure Draft are summarized as follows.

I. Improving the legal liability system for violations to the general provisions of network operation security

Article 21, Paragraph 1 and Paragraph 2 of Article 22, Article 23, Paragraph 1 of Article 24, Article 25, Article 26 and Article 28 of the Cybersecurity Law regulate the obligations to be observed by network operators, including: (1) graded systems for cybersecurity protection; (2) obligations to ensure that network products and services satisfy the mandatory requirements set forth in the applicable national standards and other duties for security protection; (3) obligations to pass the security certifications or security tests for critical network equipment and special-purpose cybersecurity products; (4) obligations to conduct real-identity authentication; (5) obligations to develop and comply with emergency plans for cybersecurity events; (6) obligations to comply with the applicable national regulations when releasing cybersecurity information such as system bugs, computer viruses, network attacks and intrusions; and (7) obligations to provide technical support and assistance to the relevant government departments in their attempts to safeguard national security and investigate crimes.

The Exposure Draft revises the penalties for violations of such provisions, including the following major changes:

2 CAC issued the Decision of Amending the Cybersecurity Law of the People's Republic of China (Exposure Draft), http://www.cac.gov.cn/2022-09/14/c_1664781649609823.htm

1. **New types of administrative penalties added for illegal conduct by network operators.** These include the circulation of notices of criticism, orders to suspend the relevant business or stop its operation for rectification, the shutdown of websites, and the revocation of relevant business permits or licenses.

2. **Raising the amount of fines imposed on network operators, supervisors directly in charge and other directly liable persons.** Where a network operator commits any of the foregoing violations and refuses to make rectifications, the fine shall be adjusted from the original "a fine ranging from CNY 10,000 to CNY 100,000" to "a fine of not more than CNY 1 million"; and for supervisors directly in charge and other directly liable persons, the fines shall be increased from "a fine ranging from CNY 5,000 to CNY 50,000" to "a fine ranging from CNY 10,000 to CNY 100,000".

3. **New penalties imposed in particularly severe circumstances.** Under particularly severe circumstances, network operators shall be subject to a fine of not less than CNY 1 million but not more than CNY 50 million or less than 5% of its turnover in the previous year, and supervisors directly in charge and other directly liable persons shall be subject to a fine of not less than CNY 100,000 but not more than CNY 1 million, and may be prohibited from serving as directors, supervisors or senior executives of related enterprises or holding any key posts relating to cybersecurity and network operation for a certain period of time.

4. **Penalty provisions added to articles without corresponding penalties in the Cybersecurity Law,** including Article 23 and Article 28.

5. **Regarding the protection of network operation security, the Exposure Draft updates the legal liability for violations of Article 27 of the Cybersecurity Law.** Article 27 of the Cybersecurity Law provides that no individual or organization may engage in activities that threaten cybersecurity, such as unlawful intrusion into others' networks, interfering with the normal functions of others' networks and stealing network data, nor provide any technical support or assistance to others that are engaged in such activities. Based on the original provisions regarding legal liability, the Exposure Draft introduces punitive measures against organizations and employment restrictions against personnel engaging in the above-mentioned activities.

II. Amending the legal liability regarding the security protection of critical information infrastructure

Articles 33, 34, 36 and 38 of the Cybersecurity Law regulate the security requirements for the construction of critical information infrastructure, the security protection obligations of critical information infrastructure operators, the security and confidentiality obligations for the procurement of critical information infrastructure, and the obligations of regular security inspection and evaluation of critical information infrastructure. The Exposure Draft amends the legal liabilities for the violation of the above provisions, which are reflected in the

following ways:

1. **New types of administrative penalties added to the illegal activities of critical information infrastructure operators.** These include the circulation of notices of criticism, orders to suspend the relevant business or stop its operation for rectification, the shutdown of websites, and the revocation of relevant business permits or licenses.

2. **Abolishing the minimum fine for refusing to make rectifications.** The fine amount has been adjusted from "a fine ranging from CNY 100,000 to CNY 1 million" to "less than CNY 1 million", and the lower limit of the fine is abolished.

3. **Adding penalty provisions under particularly serious circumstances**. The specific provisions are consistent with the aforementioned penalty provisions for network operators who violate the general provisions regarding network operation security.

4. **Transmitting the penalty provisions for violating the obligations of outbound data transfers.** Article 37 of the Cybersecurity Law requires that the operators of critical information infrastructure shall store the personal information and important data collected and generated during its operation within the territory of the People's Republic of China inbound. Where such information and data must be provided abroad for business purposes, security assessments shall be conducted. With respect to the legal liability for the violation of these obligations, the Exposure Draft stipulates that "punishments shall be imposed in accordance with the relevant laws and administrative regulations". Specifically, the operators of critical information infrastructure shall be punished according to Article 46 of the Data Security Law if they provide important data to overseas parties in violation of the aforesaid provisions; and if the operators provide personal information to overseas parties in violation of the aforesaid provisions, they shall be punished according to Article 66 of the Personal Information Protection Law.

III. Adjusting the legal liability for network content security

The Exposure Draft revises the penalty provisions of Article 47 to Article 49 of the Cybersecurity Law. The preceding provisions specify the obligations of network operators regarding network content security, which includes the timely deletion of illegal information published or transmitted by users, the prohibition of installing malware in the electronic information sent or the applications provided, and the establishment of network information security complaints and reporting mechanisms. The revisions to the corresponding penalty provisions in the Exposure Draft include the following:

1. Adding the administrative penalty of "circulating a notice of criticism" to network operators who violate the obligation for protecting network information security;

2. Raising the maximum fine from the original "CNY 500,000" to "CNY 1,000,000" for those who refuse to make rectifications or in severe circumstances;

3. Increasing the penalty provisions for particularly severe circumstances, which are consistent with the penalty provisions for network operators who violate the general provisions for network operation security;

4. The fines for relevant individuals and organizations have been increased in Paragraph 2, Article 12 of the Cybersecurity Law, which prohibits using networks to publish or transmit information about illegal activities, and Article 46, which prohibits the establishment of websites or online communication groups for the purpose of committing crimes or publishing illegal information.

IV. Amending the legal liability for personal information protection

The Exposure Draft revises the legal liability for violations of Paragraph 3 of Article 22 and Articles 41 to 44 of the Cybersecurity Law. These articles involve the requirements for network operators in the protection of personal information, including following the principles of lawfulness, legitimacy and necessity in the collection and use of personal information, the obligation to take necessary measures to ensure the security of personal information, and the obligation to respond to individuals' requests to delete or correct personal information. The Cybersecurity Law sets forth detailed provisions on legal liabilities for the violation of the aforesaid provisions. However, given that the Personal Information Protection Law provides a comprehensive legal liability system for the protection of personal information, in order to better connect with the Personal Information Protection Law, the Exposure Draft revises the original personal information protection legal liability into transitive provisions.

V. Summary

The Exposure Draft does not add any specific compliance obligations on network operators. Instead, it sets out stricter provisions on the legal liabilities of network operators (including critical information infrastructure operators) with respect to network operation security, network content security and personal information protection. For example, network operators shall be subject to a fine of up to 5% of the previous year's turnover and the supervisors directly in charge and other directly liable persons shall be subject to a fine of up to CNY 1 million as well as employment restrictions for a certain period, which will greatly increase the compliance risks and costs to network operators and management personnel. The above changes reflect the latest provisions of the Personal Information Protection Law and the regulatory trend indicated by law enforcement cases.

We recommend that enterprises focus on the amendments to the Cybersecurity Law and conduct compliance self-examinations based on the relevant requirements, to ensure that they perform their statutory obligations in accordance with the latest requirements.

Marissa DONG	Partner	Tel: 86 10 8519 1718	Email: dongx@junhe.com
Jinghe GUO	Associate	Tel: 86 10 8553 7947	Email: guojh@junhe.com
Jia ZHOU	Associate	Tel: 86 21 2208 6119	Email: zhouj_lark@junhe.com
Feng YIN	Associate	Tel: 86 10 8519 1297	Email: yinf@junhe.com