

Legal Commentary

September 24, 2022

A Brief Overview of the Draft Amendment to the Cybersecurity Law

Authors: Kevin DUAN | Kemeng CAI | Jin JIN

Introduction

On September 14, 2022, the Cyberspace Administration of China (the “**CAC**”) released an exposure draft of the *Decision on Amending the Cybersecurity Law of the People’s Republic of China (Draft for Comment)* (the “**Draft**”). In general, the Draft would impose more stringent legal liabilities for certain violations of the Cybersecurity Law (the “**CSL**”) and systematically consolidate and unify penalties for violating security protection obligations relating to network operations, network information, critical information infrastructure (“**CII**”), and personal information. The Draft would also coordinate with the Personal Information Protection Law (the “**PIPL**”), the Data Security Law, and other new laws. We briefly summarize the key points of the Draft below.

Stricter legal liabilities for violating network operation security obligations

The Draft would consolidate and unify liabilities for violating various general provisions on network operation security, including security protection obligations required by the Multi-level Protection Scheme, obligations to develop and implement emergency plans for network security incidents, and obligations to provide continuous security maintenance of products and services. Compared to the current CSL, the Draft would supplement the penalties for violating Article 23, which requires security certification or security testing for critical network equipment and special cybersecurity products. Notably, liabilities for violating these provisions would be made more stringent. The Draft echoes Article 66 of the PIPL by raising the maximum fine for personal information processors to RMB 50 million or five percent of their previous year’s turnover. The Draft would also raise the maximum fines for persons directly liable to up to 1 million yuan and add the penalty of prohibiting such persons from taking management or key cybersecurity protection positions.

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|---|--|--|
| <p>Article 21 The State adopts Multi-level Protection Scheme, under which network operators are required to perform the following obligations of security protection to ensure that the network is free from interference, disruption or unauthorized access, and prevent network data from being disclosed, stolen or tampered: 1. Formulating internal security management systems and operation instructions to determine the person in charge of cybersecurity and define accountabilities for cybersecurity; 2. Taking technical measures to prevent computer virus, network attacks, network intrusions and other activities that endanger cybersecurity; 3. Taking technical measures to monitor and record network operation and cybersecurity events, and maintaining the cyber-related logs for no less than six months as required; 4. Taking such measures as data classification, and backup and encryption of important data, etc.; and 5. Performing other obligations provided for in relevant laws and administrative regulations.</p> | <p>【Liabilities for violating network operation security】</p> <p>The competent authority shall warn such operator and order it to make rectifications. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on such operator if it refuses to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 5,000 to 50,000 yuan shall be imposed on the supervisor directly in charge.</p> | <p>【Liabilities for violating network security protection】</p> <p>The competent authority shall warn such operator and order it to make rectifications. A fine of up to 1 million yuan shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be concurrently imposed by the competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.</p> <p>For any illegal act specified in the preceding paragraph with particularly serious circumstances, the competent authority at or above the provincial level shall order it to make rectifications, and impose a fine ranging from 1 million to 50 million yuan or not more than 5% of its turnover in the previous year, and may also order it to suspend relevant business or suspend business for rectification, shutdown of website, and revocation of relevant business permit or business license; a fine</p> |
| <p>Article 25 Network operators shall develop an emergency plan for cybersecurity events to promptly respond to such security risks as system bug, computer virus, network attacks and intrusions. For an event that threatens cybersecurity, the operator concerned shall forthwith initiate the emergency plan, take corresponding remedial actions, and report as required such event to competent authority concerned.</p> | | |
| <p>Article 33 A critical information infrastructure shall be developed with the capacity to support the steady and continuous business operation, and technical security measures shall be</p> | <p>【Liabilities for CII who violates network operation security obligations】</p> <p>The competent authority shall</p> | |

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|--|---|---|
| <p>planned, established and put into use simultaneously.</p> | <p>warn such operator and order it to make rectifications. A fine ranging from 100,000</p> | <p>ranging from 100,000 yuan to 1 million yuan</p> |
| <p>Article 34 In addition to those provided in Article 20 hereof, the operator of a critical information infrastructure shall also fulfill obligations of security protection as follows: 1. Set up a dedicated security management body and designate a person in charge, and review the security backgrounds of the said person and those in key positions; 2. Provide practitioners with regular cybersecurity education, technical training and skill assessment; 3. Make disaster recovery backup of important systems and databases; 4. Work out an emergency plan for cybersecurity events and carry out drills regularly; and 5. Perform other obligations provided for in relevant laws and administrative regulations.</p> | <p>yuan to 1 million yuan shall be imposed on such operator if it refuses to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge.</p> | <p>shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to prohibit the said persons from taking positions of directors, supervisors, senior executives or key cybersecurity and network operation positions.</p> |
| <p>Article 36 The operator of a critical information infrastructure shall, in purchase of network products and services, enter into an agreement with the product/service provider in which obligations and responsibilities of security and confidentiality shall be specified.</p> | | |
| <p>Article 38 The operator of a critical information infrastructure shall conduct, by itself or entrusting a cybersecurity service provider, examination and assessment of its cybersecurity and potential risks at least once a year, and submit the examination and assessment results as well as improvement measures to the competent authorities in charge of the security of the critical information infrastructure.</p> | | |
| <p>Article 22 Paragraph 1 & 2 Network products and services shall satisfy the</p> | <p>【Liabilities for violating</p> | |

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|---|--|-----------------------------|
| <p>mandatory requirements set forth in applicable national standards. Any provider of network products or services shall not install malwares. For any risk such as security defect or bug that is found, the provider concerned shall, as required, immediately take remedial actions, inform the users of the said risk, and report the case to the competent authority.</p> <p>A provider of network products or services shall also provide consistent security maintenance for its products or services. Such maintenance shall not be discontinued within the prescribed term or the term agreed upon by the parties thereto.</p> | <p>network product and service security obligations】</p> <p>The competent authority shall give a warning and an order of rectification. A fine ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge.</p> | |
| <p>Article 48 Paragraph 1 Electronic information sent and applications provided by any individual and organization shall be free of malwares and information that are prohibited by laws and administrative regulations from release or transmission.</p> | | |
| <p>Article 24 Network operators shall require the users to provide their real identity information when signing agreements or confirmations on the provision of such services as network access, domain name registration, fixed phone and mobile phone network access, or information release and instant communication. In case that a user does not provide his/her real identity information, no network operator may provide related services for the user.</p> | <p>【Liabilities for violating user identification obligation】</p> <p>The competent authority shall order such operator to make rectifications. A fine ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or of severe circumstance, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be imposed by competent authority. A fine ranging from 10,000 yuan to 100,000 yuan</p> | |

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|--|---|-----------------------------|
| | <p>shall be imposed on the supervisor directly in charge and other directly liable persons.</p> | |
| <p>Article 26 Activities such as cybersecurity authentication, testing, and risk assessment, and releasing of cybersecurity information such as system bug, computer virus, network attacks and intrusions shall be carried out in compliance with applicable regulations of the State.</p> | <p>【Liabilities for illegally operating network service】 The competent authority shall warn such operator and order it to make rectifications. A fine of ranging from 10,000 yuan to 100,000 yuan shall be imposed in case of refusal to make rectifications or severe circumstance, and further penalties such as suspension of related business, winding up for rectification, close of website, and revocation of business license may be imposed by the competent authority. A fine ranging from 5,000 yuan to 50,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.</p> | |
| <p>Article 23 Under the compulsory requirements set forth in national standards, critical network equipment and special-purpose cybersecurity products shall not be sold or supplied until such equipment or product successfully passes security certification or security tests by a qualified organization. CAC shall work with departments concerned of the State Council to formulate and release a catalogue of critical network equipment and special-purpose cybersecurity products, and promote mutual recognition of security certificate and security test results for the avoidance of repeated certification and tests.</p> | <p>Liabilities not stipulated</p> | |

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|--|---|--|
| <p>Article 28 Network operators shall provide public security organs and national security authorities with technical support and assistance in their attempts to safeguard national security and investigate into crimes.</p> | <p>【Liabilities for refusing to assist in maintaining national security and investigating into crimes】</p> <p>Shall be warned and ordered by the competent authority to make rectifications. A fine of ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or severe violations and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.</p> | |
| <p>Article 27 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' network and stealing network data, provide programs or tools for such intrusions, interference or stealing, or provide any assistance such as technical support, advertisement, payment or settlement for any other person if the individual or organization is fully aware that such person engages in an activity endangering cybersecurity.</p> | <p>【Liabilities for threatening network security】</p> <p>While not constituting a crime, it shall be subject to confiscation of illegal earnings and detention of less than 5 days by the public security authority and a fine ranging from 50,000 yuan to 500,000 yuan. Severe violation in this regard shall be subject to a detention of above 5 days but below 15 days and a fine ranging from 100,000 yuan to 1 million yuan.</p> <p>Any organization the conduct mentioned in the preceding paragraph shall be subject to confiscation of illegal earnings by the public security authority and a fine ranging from 100,000 yuan to 1 million yuan. The supervisor directly in charge and other directly liable persons shall be subject to penalty prescribed in the preceding paragraph.</p> | <p>【Liabilities for causing severe damage to network security】</p> <p>While not constituting a crime, it shall be subject to confiscation of illegal earnings and detention of less than 5 days by the public security authority and a fine ranging from 50,000 yuan to 500,000 yuan. Severe violation in this regard shall be subject to a detention of above 5 days but below 15 days and a fine ranging from 100,000 yuan to 1 million yuan.</p> <p>Any organization the conduct mentioned in the preceding paragraph shall be subject to confiscation of illegal earnings by the public security authority and a fine ranging from 100,000 yuan to 1 million yuan. The supervisor</p> |

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|---|--|--|
| | <p>Any person who violates Article 27 hereof and receives public security administrative punishment shall not be allowed to hold key posts of cybersecurity and network operation for 5 years, and any such person who receives criminal punishment shall not be allowed to hold key posts of cybersecurity and network operation for his/her lifetime.</p> | <p>directly in charge and other directly liable persons shall be subject to penalty prescribed in the preceding paragraph.</p> <p>Any person who violates Article 27 hereof and receives public security administrative punishment shall not be allowed to hold key posts of cybersecurity and network operation for 5 years, and any such person who receives criminal punishment shall not be allowed to hold key posts of cybersecurity and network operation for his/her lifetime.</p> |
| <p>Article 46 Any individual or organization is responsible for his/its use of network, and shall neither establish any website or online communication group for the purpose of conducting fraud, transmitting criminal methods, making or selling prohibited or controlled items, or conducting other illegal criminal activities nor utilize the network to release information involving implementation of fraud, making or sales of prohibited or controlled items, and any other illegal criminal activity.</p> | <p>【Liabilities for committing crimes through use of network】</p> <p>If such violation does not constitute a crime, such individual or organization shall be subject to detention of less than 5 days by the public security authority and a fine ranging from 10,000 yuan to 100,000 yuan. Severe violation in this regard shall be subject to a detention of more than 5 days but less than 15 days and a concurrent fine ranging from 50,000 yuan to 500,000 yuan. The website or online communication group involved in the violation shall be closed.</p> <p>Those units with the conduct mentioned in the preceding paragraph shall be subject to a fine ranging from 100,000 yuan to 500,000 yuan by the public security authority. The supervisor directly in charge and other directly liable persons shall be subject to penalty prescribed in the preceding paragraph.</p> | <p>directly in charge and other directly liable persons shall be subject to penalty prescribed in the preceding paragraph.</p> <p>Any person who violates Article 27 hereof and receives public security administrative punishment shall not be allowed to hold key posts of cybersecurity and network operation for 5 years, and any such person who receives criminal punishment shall not be allowed to hold key posts of cybersecurity and network operation for his/her lifetime.</p> |

Align with the PIPL on liabilities for violating personal information rights

Prior to the effective date of the PIPL (November 1, 2021), the competent authorities mainly imposed administrative penalties for violations of personal information rights based on provisions in the CSL. Naturally, after the PIPL came into force, liabilities related to personal information protection in the CSL should be consistent with the PIPL to avoid any conflict in their application. The Draft would replace the penalty provisions in the current CSL on violating personal information rights with provisions that refer to the PIPL and other applicable laws and administrative regulations. On the one hand, the Draft retains the penalties that conform to related provisions of the PIPL. On the other hand, compared to the current CSL, the Draft would toughen legal liabilities for violations of personal information rights.

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|--|--|---|
| <p>Article 22 Paragraph 3 A provider of network products or services shall expressly notify and obtain consent of the users if the products or services collect user information; and if personal information of users are involved, the provider shall also comply with provisions of the present Law and the relevant laws and administrative regulations governing protection of personal information.</p> | <p>【Liabilities for violating personal information rights】</p> <p>The competent authority shall order such operator or provider to make rectification and such operator or provider may be subject to one or combination of the following actions, depending on the severity of the circumstance: warning, confiscation of illegal earnings, a fine equivalent to more than 1 but less than 10 times the illegal earnings, or a fine less than 1million yuan and the supervisor directly in charge and other directly liable persons subject to a fine ranging from 10,000 yuan to 100,000 yuan if there is no illegal earnings. In case of severe violation, the competent authority may order suspension of related business, winding up for rectification, shutdown of website, and revocation of business license of such operator or provider.</p> | <p>【Liabilities for violating personal information rights】</p> <p>Shall be subject to penalties pursuant to applicable laws and administrative regulations.</p> |
| <p>Article 41 Network operators shall abide by the “lawful, justifiable and necessary” principles to collect and use personal information by announcing rules for collection and use, expressly notifying the purpose, methods and scope of such collection and use, and obtain the consent of the person whose personal information is to be collected.</p> <p>No network operator may collect any personal information that is not related to the services it provides. It shall collect and use, and process and store personal the information in the light of laws and administrative regulations and agreement with the users.</p> | | |
| <p>Article 42 No network operator may disclose, tamper with or destroy personal information that it has collected, or disclose such information to others without prior consent of the person whose personal information has been collected, unless such information has been</p> | | |

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|--|---|-----------------------------|
| <p>processed to prevent specific person from being identified and such information from being restored.</p> <p>A network operator shall take technical and other necessary measures to ensure the security of personal information it collects, and to protect such information from disclosure, damage or loss. In case of disclosure, damage or loss of, or possible disclosure, damage or loss of such information, the network operator shall take immediate remedies, notify the users in accordance with the relevant provisions, and report to competent authority.</p> | | |
| <p>Article 43 Each individual is entitled to require a network operator to delete his or her personal information if he or she finds that collection and use of such information by such operator violate the laws, administrative regulations or the agreement by and between such operator and him or her; and is entitled to require any network operator to make corrections if he or she finds errors in such information collected and stored by such operator. Such operator shall take measures to delete the information or correct the error.</p> | | |
| <p>Article 44 No individual or organization may steal or otherwise unlawfully obtain any personal information, or sell or unlawfully provide any personal information to others.</p> | <p>【Liabilities for violating personal information rights】</p> <p>While not constituting a crime, it shall be subject to confiscation of illegal earnings by the public security authority and a concurrent fine equivalent to more than 1 but less than 10 times the illegal earnings or a fine less than 1 million yuan if there is no illegal earnings.</p> | |

Impose stricter legal liabilities for violating cii security protection obligations

For violations of national security review requirements for procurement by CII operators, the Draft would also raise the maximum fines to five percent of the violator’s previous year’s turnover. For violations of data localization and data export requirements for CII operators, the Draft refers to Article 46 of Data Security Law and Article 66 of the PIPL, both of which impose stricter legal liabilities on CII operators.

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|--|--|--|
| <p>Article 35 Any purchase of network products and services by the operator of critical information infrastructure that may threaten the national security is subject to the national security review conducted by the CAC together with competent departments of the State Council.</p> | <p>【Liabilities for violating national security review requirement for CII procurement】</p> <p>Shall be ordered by the competent authority to stop such use and shall be subject to a fine equivalent to more than 1 but less than 10 times the purchase price, and the supervisor directly in charge and other directly liable persons shall be subject to a fine of ranging from 10,000 yuan to 100,000 yuan.</p> | <p>【Liabilities for violating national security review requirement for CII procurement】</p> <p>Shall be ordered by the competent authority to stop such use and shall be subject to a fine equivalent to more than 1 but less than 10 times the purchase price or not more than 5% of its turnover of the previous year, and the supervisor directly in charge and other directly liable persons shall be subject to a fine of ranging from 10,000 yuan to 100,000 yuan.</p> |
| <p>Article 37 The operator of a critical information infrastructure shall store within the territory of the People’s Republic of China personal information and important data collected and generated during its operation within the territory of the People’s Republic of China. Where such information and data have to be provided abroad for business purpose, security assessment shall be conducted pursuant to the measures developed by the CAC together with competent departments of the State Council, unless otherwise provided for in laws and administrative regulations, in which such laws and administrative regulations shall prevail.</p> | <p>【Liabilities for violating CII data storage and export requirement】</p> <p>Shall be warned and ordered by the competent authority to make rectifications, and shall be subject to confiscation of illegal earnings and a fine ranging from 50,000 yuan to 500,000 yuan, and may be subject to suspension of related business, winding up for rectification, shutdown of website, and revocation of business license, and the supervisor directly in charge and other directly liable</p> | <p>【Liabilities for violating CII data storage and export requirement】</p> <p>Shall be subject to penalties pursuant to applicable laws and administrative regulations.</p> |

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|------------------|--|-----------------------------|
| | persons shall be subject to a fine ranging from 10,000 yuan to 100,000 yuan. | |

Integrate liabilities for violating network information security obligations

The Draft integrates liabilities for violating network information security obligations, including user information governance, security management, and the establishment of network information security complaint and reporting systems. Similar to the aforementioned sections, the Draft raises the maximum fine to 50 million yuan or five percent of the violator’s previous year’s turnover and adds a prohibition on directly liable persons from taking management or key cybersecurity protection positions.

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|---|--|---|
| <p>Article 48 Paragraph 1 Electronic information sent and applications provided by any individual and organization shall be free of malwares and information that are prohibited by laws and administrative regulations from release or transmission.</p> | <p>【Liabilities for providing malicious programs in the network】</p> <p>The competent authority shall give a warning and an order of rectification. A fine ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or in case of consequential severe damage to the network, and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge.</p> | <p>【Liabilities for violating information security management obligations】</p> <p>The competent authority shall warn such operator and order it to make rectifications, and shall confiscate its illegal earnings. A fine up to 1 million yuan shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be concurrently imposed by the competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.</p> <p>For any illegal act specified in the preceding paragraph with particularly serious circumstances, the competent authority at or above the provincial level shall order it to make rectifications, and impose</p> |
| <p>Article 47 A network operator shall strengthen the management of the information released by its users. If it finds any information that is prohibited by laws and administrative regulations from release or transmission, it shall immediately cease transmission of such information, and take measures such as deletion to prevent dissemination of such information. The operator shall also keep relevant record, and report the case to the competent</p> | <p>【Liabilities for violating information security management obligations】</p> <p>The competent authority shall warn such operator and order it to make rectifications, and shall confiscate its illegal earnings. A fine of ranging from 100,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or severe violations, and further</p> | |

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|--|--|---|
| <p>authority.</p> <p>Article 48 Paragraph 2 Providers of electronic information transmission service and application download service shall assume the obligations of security management. If any such provider becomes aware that its user engages in any act mentioned in the preceding paragraph, such provider shall immediately stop providing such service, take measures such as deletion, keep the record, and report to competent authority.</p> | <p>penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be concurrently imposed by the competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.</p> | <p>a fine ranging from 1 million to 50 million yuan or not more than 5% of its turnover of the previous year, and may also order it to suspend relevant business or suspend business for rectification, shutdown of website, and revocation of relevant business permit or business license; a fine ranging from 100,000 yuan to 1 million yuan shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to prohibit the said persons from acting as directors, supervisors, senior executives or holding key posts of cybersecurity and network operation.</p> |
| <p>Article 49 A network operator shall establish network information security complaint and reporting mechanisms, and shall release the complaint and reporting channels to promptly accept and settle complaints and reports concerning network information security.</p> <p>Network operators shall cooperate with the Cyberspace administration and any other competent authority in their lawful inspections and supervisions.</p> | <p>【Liabilities for hindering enforcement of competent authorities】</p> <p>Shall be warned and ordered by the competent authority to make rectifications. A fine of ranging from 50,000 yuan to 500,000 yuan shall be imposed in case of refusal to make rectifications or severe violations and a fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.</p> | <p>【Liabilities for release or transmission of prohibited information】</p> <p>Shall be subject to penalties pursuant to applicable laws and administrative regulations.</p> <p>Where there are no provisions on such cases, the competent authority shall warn such operator and order it to make rectifications, and shall confiscate its illegal earnings.</p> |
| <p>Article 12 Paragraph 2 Individuals and organizations using the network shall comply with the Constitution and laws, follow the public order, and show respect for social moralities, and shall neither impair cybersecurity nor engage in activities, by making use of the network, that endanger national security, honor and interests, incite subversion of the state power or overthrow of the socialist system, incite splitting of the country,</p> | <p>【Liabilities for release or transmission of prohibited information】</p> <p>Shall be subject to penalties pursuant to applicable laws and administrative regulations.</p> | <p>【Liabilities for release or transmission of prohibited information】</p> <p>Shall be subject to penalties pursuant to applicable laws and administrative regulations.</p> <p>Where there are no provisions on such cases, the competent authority shall warn such operator and order it to make rectifications, and shall confiscate its illegal earnings.</p> |

| Related articles | Liabilities under the CSL | Liabilities under the Draft |
|---|---------------------------|--|
| <p>undermine national unity, advocate terrorism and extremism, ethnic hatred and discrimination, spread violent and pornographic information, fabricate and disseminate false information to disrupt economic and social orders, or infringe upon the reputation, privacy, intellectual property and other legitimate rights and interests of others.</p> | | <p>A fine up to 1 million yuan shall be imposed in case of refusal to make rectifications or severe violations, and further penalties such as suspension of related business, winding up for rectification, shutdown of website, and revocation of business license may be concurrently imposed by the competent authority. A fine ranging from 10,000 yuan to 100,000 yuan shall be imposed on the supervisor directly in charge and other directly liable persons.</p> <p>For any illegal act specified in the preceding paragraph with particularly serious circumstances, the competent authority at or above the provincial level shall order it to make rectifications, and impose a fine ranging from 1 million to 50 million yuan or not more than 5% of its turnover of the previous year, and may also order it to suspend relevant business or suspend business for rectification, shutdown of website, and revocation of relevant business permit or business license; a fine ranging from 100,000 yuan to 1 million yuan shall be imposed on the person directly in charge and other directly liable persons, and a decision may be made to prohibit the said persons from acting as directors, supervisors, senior executives or holding key posts of cybersecurity and network operation.</p> |

Conclusion

The Draft mainly focuses on imposing stricter liabilities for violations of the CSL and conforming to the PIPL on the maximum penalties of both the company and persons directly liable, thereby reflecting China's strong attitude toward cybersecurity protection. The Draft is currently open for public comments and there remains significant time before it may enter into force. Therefore, parties who engage in network operations should continue to actively fulfill their obligations relating to network operation security, network information security, and personal information protection, and monitor this and other legislative developments.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123

Email: kevin.duan@hankunlaw.com

Kemeng CAI

Tel: +86 10 8516 4289

Email: kemeng.cai@hankunlaw.com