Legal Commentary

August 18, 2020

HAN KUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG

Brief Comments on the Draft Data Security Law

Authors: Kevin DUAN | Kemeng CAI | Shasha ZHOU | Minzhe HU

Since October 2019, the Central Committee of the Communist Party of China and the State Council have successively issued documents clarifying the status of data as a new production factor, demanding acceleration of the cultivation of the data element market, promotion of the publication and sharing of government data, and enhancement of the value of social data resources, and, through unified legislation, further providing basic safeguards for data protection and giving full play to the value of data as a production factor. Furthermore, as data also becomes an increasingly prominent strategic resource with the continued development of the digital economy, many issues unique to the digital age, such as data sovereignty, cross-border data transfers, and data-related trade controls, require legislative clarity so as to better protect national security and state interests.

On June 28, the Standing Committee of the National People's Congress for the first time deliberated and published the full text of the closely-watched *Data Security Law of the People's Republic of China (Draft)* (the "**Draft Law**"). The Draft Law summarizes, refines, and adopts into law the requirements for data governance that have been implemented in practice in recent years, and outlines the future institutional framework for data security protection in China. We believe that the Draft Law is highly notable in the following aspects:

Scope of application

According to its provisions, the Draft Law governs data activities undertaken in China, including data collection, storage, processing, use, provision, transactions, and disclosure. In addition, the Draft Law also stipulates certain extraterritorial effect, i.e. offshore organizations and individuals are held liable for engaging in data activities that harm China's national security, public interests, or the legitimate rights and interests of Chinese citizens and organizations.

The Draft Law also further stipulates that, with respect to specially protected data such as data involving state secrets and personal information, the special provisions under the Law on Guarding State Secrets and personal information protection laws shall prevail.

Division of responsibilities for data security and protection

The Draft Law specifies responsibilities and duties of the central and local governments in terms of data security and protection.

1. **Central government level**: the central national security leadership department, i.e. the National Security Council, will be responsible for the decision-making and overall coordination of China's data security work; the Cyberspace Administration of China will be responsible for overall coordination of network data security and protection and related supervision work; national public security organs and national security organs shall be responsible for data security and supervision according to their respective duties.

2. **Local and departmental level**: local departments and each ministry will undertake primary responsibility for the data generated, aggregated, and processed in the execution of their respective work duties and are to be responsible for data security.

3. **Industry level**: competent industry authorities will be responsible for unified data security supervision in sectors such as industrial, telecommunications, natural resources, health, education, defense technology industry and financial.

The foregoing data administration system emphasizes centralized leadership while also accounting for the features of data administrative practice in various regions and industries. This would allow for departments to administer various industries and for governments in different regions to implement distinct data protection regimes adaptive to characteristics of these industries and regions under the guidance of national principles and guidelines.

Data classification and categorization and protection of important data

In terms of data security administration, the Draft Law stipulates requirements for classified and categorized data protection, emphasizing that special efforts should be made to protect "important data." Before the promulgation of the Draft Law, authorities had put forward requirements for data classified and categorized protection for important areas such as finance, electricity, healthcare, and critical infrastructure. The Draft Law continues to use the data classification standards applicable for the network data protection, and proposes to implement classified data protection based on the degree of harm caused to national security, public interests, or the legitimate rights and interests of Chinese citizens and organizations if the relevant data is tampered with, destroyed, disclosed, or illegally obtained or used.

On the basis of data classified protection, the Draft Law further proposes basic requirements for important data protection, including:

1. Important data processors are to establish responsible persons and management organizations in charge of data security and implement duties for data security and protection;

2. Important data processors are to carry out risk assessments in accordance with regulations and submit risk assessment reports to relevant competent authorities, which should specify the types and quantities of important data which the processor holds, the circumstances related to data collection,

storage, processing, and use, and potential data security risks and countermeasures, etc.

According to the 2019 *Measures for Administration of Data Security (Draft for Comment)*, important data is defined as "data that, once disclosed, may directly influence national security, economic security, social stability, and public health and safety", such as data concerning undisclosed government information, large-scale population, genetic health, geographic and mineral resource, etc. Important data generally does not include enterprise production, operation and internal management information, personal information, and so on. The Draft Law does not clearly define important data, likely due to the broad types of important data, instead authorizing local and industry competent authorities to formulate important data protection catalogues corresponding to the features of their respective regions and industries. However, it remains to be observed how conflicts will be resolved between the definitions of important data which these competent authorities formulate in practice.

Data transaction system

In recent years, data exchanges have been established in Guiyang, Shanghai, Wuhan, Chongqing, etc., and data transaction partnerships have become important data sources for market players in fields such as financial risk control and credit investigation, advertising media, map surveying and mapping, health and medicine, environment and meteorology. The Draft Law proposes a breakthrough by officially recognizing under law the legal status of data transactions and data transaction service providers[1]. Key provisions include:

1. Article 3 acknowledges data transactions as a data activity and entitles proper legal status to data transaction activities;

2. Article 17 stipulates that the government is to establish and improve a data transaction system, regulate data transaction behaviors, and cultivate data transaction markets;

3. Article 30 stipulates that "agencies engaged in data transaction intermediary services" require data providers to explain the sources of the data, verify the identities of both parties to transactions, and preserve corresponding review and transaction records;

4. Article 43 stipulates that if a data transaction intermediary agency fails to fulfill its obligations under Article 30 which causes a data transaction to originate from illegal sources, the relevant competent authority will order the agency in violation to make corrections, confiscate illegal income gained, and impose administrative penalties, which includes imposing fines, revoking business operating licenses and business licenses, etc. A fine is also to be imposed on the responsible person of the agency in violation.

Considering the complexity and diversity of data transaction deals, as well as debate remaining over the ownership of data at the jurisprudence level, the Draft Law does not elaborate on data transaction system, but leaves it to be further explored in practice based on specific data types and application scenarios. However, since the Draft Law formally recognizes under law the legal status of data transactions, we can

[1] To some extent, *General Provisions of the Civil Law*, promulgated in 2017, recognizes data as being subject to property protections and lays the foundation for the data transaction system.

foresee that it will bring vitality to various industries in the future.

Data security review system

Article 22 of the Draft Law stipulates for the first time China's data security review system, with the aim to establish a comprehensive cyberspace and data security protection system, further safeguard China's cyberspace sovereignty, and prevent disclosure and destruction of data and information that may influence national security. The Draft Law does not specify the concepts of the data security review system, but in principle requires that data activities be subject to a national security review if the data activities may influence national security. We understand that because the data security review system would apply to all data activities within China, that it may also in the future cover the closely-watched cross-border data security review system. In addition, according to the Draft Law, decisions of administrative departments on data security reviews may be final and are not subject to existing remedies such as administrative reconsideration litigation, signifying the discretion and specialization administrative departments have regarding this issue.

Clarifies data sovereignty and promotes cross-border data flows

Security assessments of cross-border data transfers continue to be a closely watched issue. Rather than prescribing specific rules related to cross-border data transfer security assessments, the Draft Law provides for export controls related to cross-border data transfers, data use-related countermeasures, and a reporting and approval system for cross-border data enforcement. These provisions manifest China's fundamental vision for safeguarding data security and encouraging the free flow of data. On one hand, data is a key element for digital economic development: the Draft Law indicates China will actively participate in international data exchanges and promote cross-border data flows. On the other hand, data is also a fundamental national strategic resource: the Draft Law proposes establishing a data export control system, data-use countermeasure system, and a reporting and approval system for overseas data retrieval for purposes of safeguarding national interests and effectively responding to risks and challenges China faces in safeguarding national security in the data field.

I Strengthens cross-border data exchanges and cooperation

As the world's second largest digital economy, China has always considered the digital economy as a key sector when promoting cross-border exchanges and cooperation, and data is a key element for promoting the development of the digital economy. In order to further promote cross-border data flows, the Draft Law provides at Article 10 that China will actively promote cross-border data exchanges and cooperation, participate in the formulation of international rules and standards related to data security, and cooperate with other countries to promote cross-border data flows in a secure and free manner.

II Establishes a data export control system

Cross-border data flows give rise to issues such as how to define data sovereignty and how to protect data security. In this context, the Draft Law proposes for the first time a data export control system, i.e. to implement export controls in accordance with law for data that is categorized as controlled and

is relevant to fulfilling international obligations and maintaining national security. However, it remains to be observed how the data export control system will connect the data national security review system and cross-border data transfer security assessment system.

III Specifies countermeasures to be taken against restrictive measures on investment and trade related to data and data development and utilization

In the context of worsening trade and investment conflicts globally, the Draft Law specifies that China may take corresponding countermeasures based on actual circumstances against any country or region which adopts discriminatorily prohibitive, restrictive, or other similar measures against China in respect of investment and trade related to data development, utilization, and technologies.

IV Clarifies issues related to data retrieval in cross-border law enforcement

In terms of obtaining data in cross-border law enforcement, foreign organizations are prohibited from directly engaging in investigations and collecting evidence in China in criminal and securities matters, respectively under the *Law of the People's Republic of China on International Judicial Assistance in Criminal Affairs*, as adopted in 2018, and the *Securities Law of the People's Republic of China*, as revised in 2019. These laws specify that domestic organizations or individuals may not to submit evidence to foreign parties without the consent of the competent authorities. The Draft Law, as the basic law for the data field, further specifies that, in principle, domestic organizations and individuals must report to and seek approval from the competent authorities prior to transferring data to overseas law enforcement agencies.

Fulfills the task of government data publication

In order to promote e-government development and fulfill the task of government data publication as described under the *Action Outline for Promoting Big Data Development*, the Draft Law devotes a special chapter to rules on security and publication of government data, and further specifies a government data security management system and rules for the publication and use of government data, with a view to promote the publication and exploitation of government data resources.

In one respect, the Draft Laws stipulate basic principles for government data publication. Specifically, the government is to continue to abide by the principle of "government data should be published except in special circumstances" as prescribed under the *Regulations on Disclosure of Government Information*, and should disclose government affairs data in a timely and accurate manner by following the principles of fairness, equality, and convenience for the public. In addition, the Draft Laws stipulate the formulation of a government data publication catalog in order to build a unified, standardized, interconnected, and secure and controllable government data publication platform and to promote and implement the publication and use of government data.

In fact, to date, local governments have successively promulgated regulations on public data disclosure and secure management, and have consistently planned and improved their data disclosure platforms, for example:

1. In 2016, the Guiyang government took the lead in the construction of a data publication platform to

disclose to the public free data resources, with a scope of disclosure covering government data of all Guiyang municipal governmental departments and related directly subordinate institutions.

2. In 2018, Shanghai promulgated the *Measures of Shanghai Municipality on Administration of Public Data and One-stop Handling Networks* and the *Interim Measures of Shanghai Municipality on the Disclosure of Public Data*, to provide specific rules related to the publication procedures, platform construction, and security safeguards during the publication of public data, including government data.

3. In 2019, Beijing promulgated the *Work Plan on Disclosure of Public Data to Promote the Development of the Artificial Intelligence Industry*, proposing that Beijing will take the lead in building a data publication innovation base nationwide, and make conditional disclosure of a batch of special public data resources to Beijing artificial intelligence companies, including medical insurance data, judicial data and traffic data, with the aim to supply data in a free and accurate manner to satisfy enterprises' needs regarding product development and application innovation. The *Measures for Administration of Publication of Traffic and Travel Data (for Trial Implementation),* promulgated in the same year, stipulate the publication of traffic data for the purpose of promoting the deep integration of the transportation sector and Internet companies, and optimizing and improving travel guidance services.

4. In 2020, Zhejiang promulgated China's first provincial-level legislation on public data disclosure—the *Interim Measures of Zhejiang Province on the Public Data Disclosure and Security Management*, which comprehensively provide rules on data publication, channels of publication and data security, and further specify big data administration duties and the experts committee system.

The government data disclosure system stipulated by the Draft Law will help to make full use of government data as a public resource, and promote and deepen the intelligent and digital transformation of various industries, so as to better allow data to facilitate China's economic and social development.

Conclusion

The Draft Law provides an initial summary of the preceding stage of data governance and practices in China, and describes multiple basic systems in terms of data security and development by comprehensively considering the characteristics of the digital economy. It can be regarded as both a reasonable and necessary supplement to the *Cybersecurity Law of the People's Republic of China* in respect of cyberspace governance. The Draft Law, together with the forthcoming Personal Information Protection Law, rules for determining important data, data security review systems, and cross-border data transfers systems, not only respond to many issues which concern the public in practice, but also provide a legal basis for the development of data markets and the data industry in the future.

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