JUNHE BULLETIN

JUNHE

July 9, 2020

Hot Issues Regarding Data Protection and Cybersecurity Law

Data Security Legislation Accelerated – Draft Data Security Law Released for Public Consultation

On July 3, 2020, the text of the *Data Security Law* (Draft) ("**Draft Law**") that has attracted much attention was officially released on the website of the National People's Congress for public consultation[1] after being submitted to the 20th meeting of the Standing Committee of the 13th National People's Congress for consideration.

In the "Legislation Plan of the Standing Committee of the 13th National People's Congress" that was released in September 2018, the *Data Security Law* was included in the legislation plan for the first time as "a draft law to be submitted for deliberation during the tenure under relatively mature conditions". [2] After two years of deliberations, the text of this Draft Law has been officially released.

After its promulgation, the *Data Security Law* will become an important part of the national security legal system represented by the *National Security Law*, and will, together with the *Cybersecurity Law* and the *Personal Data Protection Law* that is being drafted, become a more complete basic legal system in the field of legislation on information.

I. Scope of Application

The Draft Law provides that this Law is applicable to data activities carried out **within** the People's Republic of China. In terms of its extraterritorial application, the Draft Law further provides that any organization or individual **outside the territory** of the People's Republic of China will be investigated for legal liability if such an organization or individual harms the national

[1] http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80808172b5fee801731385d3e429dd

[2] http://www.npc.gov.cn/npc/c30834/201809/f9bff485a57f498e8d5e22e0b56740f6.shtml

security, public interests or legitimate rights and interests of the citizens and organizations of the People's Republic of China in carrying out data activities. (*Article 2*)

The Draft Law further provides that "Data" means any record of information in electronic or non-electronic form; while "Data Activities" shall mean such acts as data collection, storage, processing, use, provision, transaction and disclosure. (*Article 3*)

According to the above definitions, "Data" covers a wide range of information generated from all aspects of production, operation and management in the process of the gradual transformation of government affairs and enterprises to digitalization. The supplementary provisions of the Draft Law further provide that Data Activities involving national security and personal data shall be governed by the *Law of the People's Republic of China on Keeping State Secrets* and the laws and regulations related to personal data respectively, therefore, the Draft Law does not include Data Activities involving state secrets, nor is it specially applicable to the data activities on personal data. However, the boundaries of the Data involved in the Draft Law, especially how to apply the Draft Law in the business practice of enterprises still needs to be defined further. For example, the Draft Law requires the protection of Data based on a hierarchical classification, and only formulates the relevant specific obligations (as set out in Part V of this Article) on important data, however, further clarification still needs to be made on whether Data other than important data are to be regulated accordingly, as well as the focus and rules of regulation.

The Draft Law provides that Data Security means the ability to ensure the effective protection and lawful use of Data and to keep the Data under a continuous security status by taking necessary measures. (*Article 3*) As seen from the entire contents of the Draft Law, Data Security mentioned therein includes both at the macro level of national security and at the micro level of the implementation of data security measures by organizations and individuals.

II. The Linkage between the Draft Law and the Legal System of Security and Cyber Affairs

Data Security is an important component of national security and cybersecurity.

The *National Security Law* provides in principle that the State will construct networks and information security safeguard systems, improve its ability to protect networks and data security, and strengthen networks and information technology innovative research and development applications, so as to realize data security and control (*Article 25*).

The *Cybersecurity Law* also requires enterprises to perform their obligations of hierarchical cybersecurity protection, take such measures as data classification, important data backup and encryption (*Article 21*). We have noticed that further observation is required for the coordination and connection of the provisions of the aforesaid laws and relevant supporting regulations (and the draft for comments), for example:

- The linkage between the relevant obligations on the protection of important data as provided in the Draft Law and those as defined and provided in the *Cybersecurity Law* and the *Data Security Administrative Measures* (Draft for Comment);

- The linkage among the Data export control system as provided in the Draft Law and the export control requirements provided in the *Export Control Law* (Second Draft for Review) that is being formulated, and the relevant requirements for data export as provided in the *Cybersecurity Law*, *Data Security Administrative Measures* (Draft for Comment) and the *Measures for Safety Evaluation of Personal Data Exit* (Draft for Comment);

- The linkage between the Data Security review system as provided in the Draft Law and the foreign investment safety review system as provided in the *Foreign Investment Law* and the *Cybersecurity Review Law;* and

- The linkage between the Data Security management system and risk monitoring on Data Activities required to be put into place by enterprises as provided in the Draft Law, and the relevant systems of grade-based security protection as provided in the *Cybersecurity Law*.

III. The Principle of Regarding Data Security and Development as Equally Important

In the general provisions, the Draft Law firstly specifies that the State protects the Data-related rights and interests of citizens and organization, encourages the rational and effective utilization of Data, secures the orderly and free flow of Data in accordance with the law, so as to promote the development of the digital economy with Data being the key element and improving the well-being of the people (*Article 5*).

Next, in the second chapter, the Draft Law expressly provides its support to Data development and utilization and regards both Data Security and the promotion of Data development and utilization as being equally important. The relevant support measures include the implementation of a Big Data strategy, the promotion of Data infrastructure construction, the design of a digital economy development plan (*Article 13*); the strengthening of basic research on Data development and utilization technology (*Article 14*); the promotion of digital talent cultivation (*Article 18*) and other general strategies and guidelines for the encouragement and support of digital economy development, digital development and utilization. It also states a requirement to formulate the relevant standards for data development and utilization technologies, products, and Data Security (*Article 15*); to promote Data Security monitoring and evaluation as well as certification (*Article 16*) and establish and improve Data transaction management systems (*Article 17*).

To sum up, in terms of its system design, the Draft Law is intended to encourage and establish various Data-related policy support measures to promote and coordinate the balanced and orderly development between the digital economy and Data Security by taking in to consideration Data management and requirements.

IV. Data Security Law Enforcement Bodies and their Work Duties

Articles 6 and 7 of the Draft Law specify the regulation of Data Security and the work duties of different law enforcement bodies. The Central State security leading institution is responsible for the decision-making and overall planning and coordination of the entire Data Security work, and formulates the general strategies and policies for Data Security. In addition:

- The various regions and departments shall have the responsibility as the subjects of the Data Activities and Data Security in the work of their own regions and departments;

- Relevant industrial departments such as industry, telecommunications, natural resources, health, education, defense-related science and technology industries, and the financial industry shall be responsible for the Data Security supervision of their own industries and fields;

- Public security organs and national security organs shall be responsible for Data Security supervision within their respective scope of duties; and

- Cyberspace administrations of the State are responsible for the overall planning and coordination of cyberspace Data Security and the relevant regulatory work.

V. The Basic System of Data Security

As the basic law in the field of Data Security, the Draft Law has established a series of fundamental systems in the field of Data Security and the basic framework of the Data Security system in China, laying a solid foundation for the development and perfection of Data Security systems in the future. These new fundamental systems include:

1. Data Protection Based on a Hierarchical Classification and Important Data Protection Systems

The Draft Law provides that the State shall protect Data based on a hierarchical classification according to the importance of Data in the economic and social development and the extent of the damage that would be caused to national security, public interest or legitimate rights and interests of citizens and organizations were the Data tampered with, destructed, disclosed or illegally obtained or used. All districts and departments shall, according to the relevant provisions of the State, determine the important data protection catalogue for its own district, department and industry and give priority to the protection of Data listed in the catalogue. (*Article 19*)

The Draft Law does not state the specific requirement for the protection of Data based on a hierarchical classification, but it imposes special requirements on the processing of important data: (1) a processor of important data shall have the responsible person and management body of Data Security (*Article 25*); and (2) a processor of important data shall make a risk assessment on the Data Activities on a regular basis, and submit the risk assessment report to the relevant administrative department. An assessment report shall include the category, quantity, storage processing and use of the important data in its possession, the imminent Data Security risks and the countermeasures. (*Article 28*)

The *Cybersecurity Law*, initially formed in 2016, mainly states the requirements on data localization and security assessment for the cross-border transmission with respect to the important data collected by critical information infrastructure operators. The relevant drafts for public consultation which are issued later enumerate and define various categories of important data, for example, the *Information Security Technology Guidelines for Security Assessment on Cross-border Transmission of Data* (Draft for Comments) and the *Data Security Administrative Measures* (Draft for Comment), and states the requirement on the processing of important data, for example, the *Data Security Administrative Measures* (Draft for Comment).

The Draft Law will establish the rules for the processing of important data, which reflects the continuous deepening of the important data management system. However, the Draft Law still does not provide a clear definition of important data, and leaves it to the districts, departments and industries to issue the relevant lists, which reflects the complexity of classifying and defining important data in practice.

2. Data Security Risk Management and Control Systems

The Draft Law requires the State to establish a unified, efficient and authoritative mechanism for Data Security risk assessment, reporting, information sharing, and monitoring and early warning, so as to strengthen the management and control of Data Security risks. (*Article 20*) The details of such a system and the obligations of the relevant governmental departments and enterprises will be provided in the relevant supporting regulations promulgated in the future.

3. Data Security Emergency Response Mechanisms

The State will establish a Data Security emergency response mechanism. In the case of a Data Security incident, the relevant administrative department shall, according to the law, launch an emergency plan and take corresponding emergency measures to eliminate hidden security hazards, prevent the expansion of damage, and issue to society in a timely manner any warning information in relation to the public (*Article 21*). The connection between the foregoing provision and the existing regulations such as the Emergency Response Law needs further observation.

4. Data Security Review

The State will establish a Data Security review system to conduct national security reviews on Data Activities that affect or may affect national security. The security review decision made according to the law shall be final. (*Article 22*)

The Draft Law does not state the details of the Data Security review system. Furthermore, the relationship between such a system and the foreign investment security review system as set out in the existing *Foreign Investment Law*, as well as the relationship between the security review system applicable to the key information infrastructure operator as set out in the *Cybersecurity Review Measures,* needs further observation.

5. Data Export Control Systems

The State shall enforce the export control systems against Data which falls into the controlled items and associates with the performance of international obligations and the safeguarding of national security according to the law. The *Export Control Law* is still under the process of stipulation. The *Export Control Law* (Second Draft for Review) released on July 20, 2020 states the requirement on the export control of goods, technologies, services and other items, and defines the export control.

Besides, the *Cybersecurity Law*, the *Data Security Administrative Measures* (Draft for Comment) and the *Measures for Security Assessment on Cross-border Transmission of Personal Information* (Draft for Comment) respectively state the requirements on security assessments on cross-border transmissions of important data and personal information by critical information infrastructure operators and network operators, but the relevant detailed rules have not yet been clarified. The coordination and connection between the data export control and the security assessment system for the cross-border transmission of Data awaits further elaboration from the future legislation.

6. Countervailing Mechanisms for Discriminatory Measures

Depending on the actual circumstances, countervailing measures shall be taken against those who take discriminatory measures against our country in aspects of investment and trade including Data and Data development and utilization technology. (*Article 24*)

VI. Obligations of Data Security Protection

Chapter 4 of the Draft Law states the obligations that entities and individuals shall fulfill under the national Data Security protection system. These basic obligations include:

- to establish and improve Data Security management systems, undertake Data Security education and training, and undertake technical security measures to carry out Data Security activities (*Article 25*);

- to monitor risks of Data Activities and report in a timely manner to the administrative department any Data Security incidents (*Article 27*);

- to obtain Data in a legal and proper manner (*Article 29*);

- to cooperate with the public security and national security authorities in retrieving Data for the purpose of safeguarding national security or investigating crimes; where an overseas law enforcement agency asks for Data that is stored within China, the entity or individual shall not provide such Data until it reports to the administrative department and obtains its approval. (*Articles 32 and 33*)

In addition to the foregoing basic obligations, the Draft Law imposes special Data Security obligations on several special subjects for their data processing activities:

- agencies engaged in the intermediary service of data trading shall ask the Data provider to explain the sources of the Data and authenticate the identity of the trading parties; in our opinion, suppliers engaged in the Data business and intermediary platforms engaged in Data business transactions need to pay full attention to such requirements (*Article 30*);

- operators providing online Data processing and other services shall obtain a business license or filing. (*Article 31*) Whether such a requirement on obtaining a license or filing as set out herein corresponds to the relevant telecommunication business license, for example, "B21 online data processing and transaction processing services" as set out in the *Telecommunication Services Catalogue*, is subject to further explanation.

VII. Government Data Openness and Security Requirements

In the context of our steady promotion of electronic government, it is vital to protect the security of government Data. On the one hand, continuous improvement of the transparency and openness of government Data is required to improve the level of social governance; on the other hand, government Data is related to national security due to its particularity, the abuse or illegal disclosure of which will endanger the State and society. Thus, Chapter 5 of the Draft Law clearly states the requirement on government Data security and openness. This includes, among others, that national authorities shall engage in Data Activities within the statutory scope of duties, establish and improve Data Security management systems, promptly and accurately announce government Data, and establish a safe and controllable open platform of government Data.

It should be particularly noted that, according to Article 37, any national authority or organization with the function of public affairs management that entrusts others to store and process government Data, or provides others with government Data, shall be subject to stringent approval procedures and shall supervise the receiving party in performing the Data Security protection obligations. Therefore, any third-party supplier that cooperates with the government or provides services to the government should pay special attention to such approval requirements. Detailed approval procedures need further observation.

VIII. Legal Liability for the Violation of Data Security Related Obligations

Chapter VI of the Draft Law sets forth the legal liabilities required to be borne for any violation of data security related obligations. It is provided for in Article 41 that the competent authority may require an interview with the relevant entity or individual if any major safety risk is found in data related activity. This chapter also specifies the legal liability to be borne respectively by any entity or individual that carries out data related activity, any data trading agent, any online data trading and other service provider, any government body or officer, or any other person, for violation of their relevant obligations under the Draft Law. It also expressly sets forth that criminal liability will be imposed on any person who has committed a criminal offence according to the law.

IX. Our Views

As the first law specific to data security in China, the Draft Law provides a legal basis and framework to set forth the basic directions and guidelines for data security protection in China.

The Draft Law involves a wide range of fields with a lot of complexity, and huge challenges may arise. A lot of issues can be foreseen in future practice, such as how to connect with the existing *Cybersecurity Law*, the *Personal Data Protection Law* being drafted and other laws and subordinate rules, how to draft and implement specific data security regulations, and how to achieve a stable and orderly development of the digital economy on the ground of data security.

Data-related activities are essential in operating a company, developing a city and running government affairs, especially with the background that big data, AI, cloud computing, blockchain and other hi-techs are growing so fast in the rising digital economy. The *Cybersecurity Law* became effective in 2017 and provided a brand-new compliance framework for the data-related activities of a company, but with a focus only on personal or important data. So far, no data security legislation covering all data has been made, and the framework for legislation and enforcement of laws governing important data are still being studied and built.

Undoubtedly, the Draft Law provides a legal basis and reference for the legal and safe use and processing of data in running enterprises and public institutions as well as government affairs, so as to ensure their internal and external data-security related compliance and perform their data security related obligations.

The players in different fields, especially finance, energy, irrigation and other key fields that may involve important data, need to pay attention to the rules and regulations governing data classification and important data protection, with a view to improving their data-security risk prevention systems and their data-security emergency response mechanisms. The transaction platforms need to improve their systems to access data sources and transaction parties. Online data processing and other service providers need to keep their eye on the future developments in the filing or permit requirements under the Draft Law. Data processing and other service providers to enterprises and public institutions will also be directly influenced by the Draft Law in terms of their future business modes and obligations.

We will keep our eye on the development of the Draft Law.

Dong Xiao	Partner	Tel: 86 10 8519 1718	Email: dongx@junhe.com
Guo Jinghe	Associate	Tel: 86 10 8553 7947	Email: guojh@junhe.com
Dong Junjie	Associate	Tel: 86 10 8540 8722	Email: dongjj@junhe.com

本文仅为分享信息之目的提供。本文的任何内容均不构成君合律师事务所的任何法律意见或建议。如您想获得更多讯息，敬请关注君合官方网站“www.junhe.com” 或君合微信公众号“君合法律评论”/微信号“JUNHE_LegalUpdates”。