China’s Draft Data Security Law Published for Public Consultation

July 20, 2020

On July 3, 2020, the Standing Committee of China’s National People’s Congress (“NPCSC”) released the first draft of the **Data Security Law of the People’s Republic of China (“Draft Law”)**.The Draft Law was published following its first reading by the National People’s Congress, and will be open for public comment until August 16, 2020. The Draft Law will then proceed through at least two additional drafting rounds before going to a vote. Although the timing of these next steps is difficult to pinpoint, many analysts predict that the law could be passed by the end of 2020.

This Client Alert identifies the Draft Law’s key provisions, and considers the implications of the Draft Law in light of other recently enacted or amended Chinese legislation: the State Secrets Protection Law (2015), Cyber Security Law (2017), International Criminal Judicial Assistance Law (2018), Securities Law (amended in 2020), and the Law on Safeguarding National Security in the Hong Kong Special Administrative Region (2020). Viewed in this context, the Draft Law is an important new piece in a series of laws geared towards safeguarding national security and asserting sovereignty and which may cause additional restrictions on information flow out of China.

Overview

The Draft Law consists of 51 articles that span seven chapters: General Provisions, Data Security and Development, Data Security System, Data Security Protection Obligations, Security and Release of Government Data, Legal Liabilities, and Miscellaneous. In the **Introductory Explanation to the Data Security Law of the People’s Republic of China Draft (“Introductory Explanation”)**, the NPCSC highlights the close connection between data security and national security, and states that “without data security, there is no national security.” This emphasis on national security is a recurring theme throughout the text of the Draft Law as described in more detail below. The Introductory Explanation also indicates the top authorities’ support for the Draft Law and for a speedy legislative process.

Key Provisions

Key elements of the draft law are summarized below:

Applicability

The Draft Law, once enacted, is intended to be generally applicable to any data activities (defined below) that take place in China (Article 2). While the extraterritorial effects of the law will be described more fully below, it is important to note from the outset that Article 2 explicitly holds individuals and foreign entities responsible for their data activities in China. The Draft Law also introduces broad definitions of data, data activities, and data security (Article 3). Data refers to any electronic or non-electronic record of information. Data activities refer to activities such as data collection, storage, processing, use, provision, transactions, and publication of data. Data security is defined as ensuring that data is effectively protected, used legitimately, and remains secure through the adoption of necessary measures.

Categorization of Data

Expansive definitions of data aside, the Draft Law acknowledges that not all data is created equal. The Draft Law stipulates that data should be categorized according to the potential harms to national security or the public interest if such data is compromised or tampered with (Article 19). Although the Draft Law does not provide a clear definition, “critical data”—a term that is also found but not defined in the Cyber Security Law—appears to receive a higher degree of scrutiny. Government authorities are tasked with creating catalogs of critical data (Article 19), and entities that process critical data are expected to designate data security managers and organs to implement additional safeguards to critical data (Article 25). These managers and organs should perform data risk assessments and report their results to the authorities (Article 28).

Responsible Authorities

The Draft Law identifies various government actors that would be involved in implementing the law. Central-level national security authorities are tasked with strategic decision-making, which would include ensuring coordination among relevant agencies as well as formulating, guiding, and implementing data security strategies and policies (Article 6). Government agencies at all levels and across different sectors are responsible for the security of the data generated, collected, and processed on their watch (Article 7). Specifically, the Draft Law holds industry, telecommunications, natural resources, public health, education, defense, and finance regulators accountable for monitoring data created in their respective domains. Public security and national security organs are responsible for ensuring data security in accordance with the authority vested in them under applicable laws. The Draft Law also identifies the Cyberspace Administration of China as the ministry responsible for ensuring and coordinating data security on the internet.

National Security and a Review System

As discussed in the Overview, national security is a consistent theme of the Draft law, and the term “national security” appears 11 times throughout (Articles 2, 4, 6, 7, 8, 22 (twice), 23, 32 (twice), and 47). Article 22 provides a basis for the establishment of a data security review system that can review any activities that influence or might influence national security data. Decisions issued by the review system will be final. This provision does not specify the criteria on which the review will be based, and we expect that subsidiary laws will be promulgated to implement this important new review system. The Draft Law also empowers the state to impose export control measures on data related to the state’s observation of international obligations or protection of national security (Article 23). If and when data activities involve state secrets, the State Secrets Law applies (Article 49). The effect appears to be a tight connection between data security and national security.

Extraterritorial Effects

The Draft Law contains a number of provisions with extraterritorial reach and cross-border effects. The Draft Law establishes extraterritorial jurisdiction over foreign entities that engage in data activities inside and outside of China that harm national security or the public interest (Article 2), and empowers the state to adopt countermeasures against countries that impose restrictive or discriminatory trade and investment safeguards against China (Article 24). Directly relevant to multinational corporations operating in China, when foreign law enforcement agencies request access to data stored in China, Article 33 requires that the individual or entity concerned must first report to and receive approval from the relevant Chinese government authorities.

Penalties

Legal liability is established in Articles 41 through 48 of the Draft Law, and the penalties range from specific to general. Article 48 allows for the imposition of administrative, civil, and/or even criminal penalties depending on the type and severity of the data security breach. Individuals and entities involved in data activities that violate Articles 25, 27, 28, and 29 of the Draft Law can be fined up to 1 million RMB for failing to correct their behavior (Article 42). For data transactions that violate Article 30 of the Draft Law and result in illegal income, the responsible data transaction intermediary can be fined up to 10 times the amount of the illegal income (Article 43). Online data processing businesses that operate without the proper licenses specified in Article 31 of the Draft Law can be fined up to 10 times the amount of their illegal income or a fine not more than 1 million RMB (Article 44). State organs, state employees responsible for data security, and those who endanger national security or the public interest would be punished according to relevant laws and regulations (Articles 45, 46, and 47).

Reading the Draft Law in Context

While some commentators have focused on the vague and generic nature of some of the Draft Law's provisions, the Draft Law is perhaps best understood in the context of other recently enacted or amended Chinese laws concerning national security and sovereignty. Read in this way, the Draft Law provides grounds for and mandates tightening control over data that is considered economically valuable or core to national security.

An Additional Procedural Barrier to Data Transfer in Response to Foreign Proceedings

First, the Draft Law seems to be the most recent piece of a procedural puzzle addressing foreign criminal proceedings or regulatory investigations concerning individuals and entities in China. The International Criminal Judicial Assistance Law ("ICJAL") stipulates that foreign authorities may not conduct criminal procedure activities in China, nor can individuals and entities in China assist those efforts without approval from government authorities (Article 4). Like the Draft Law, Article 4 of the ICJAL emphasizes that international criminal justice assistance should not harm Chinese sovereignty, national security, or the public interest. Similarly, Article 177 of the recently amended Securities Law blocks the cross-border transfer of securities business data without the approval of the China Securities Regulatory Commission. Against this backdrop, Article 33 of the Draft Law might be viewed as a catch-all provision that attempts to prevent the outflow of any data for the purposes of a foreign enforcement actions without approval from the Chinese authorities.

Systematic Regulation of Data

Second, the Draft Law reasserts the state's resolve in regulating certain types of substantive data, including critical data, state secrets, and personal information. It provides that data should be categorized according to the potential risks they pose to national security and the public interest (Article 19), and that "critical" data is especially important (Articles 19, 25, and 28). Data that qualify as "state secrets" are subject to the State Secrets Protection Law, while "personal" data are subject to the forthcoming Personal Data Protection Law (Article 49).

Cross references to other national security or data-focused legislation are also seen in the Cyber Security Law (Article 33)—with respect to critical data and personal information—and the Law on Safeguarding National Security in Hong Kong (Article 29)—with respect to state secrets. These provisions, together with standalone statutes on state secrets and personal data protection, will provide a broad basis for the state to regulate data. The connection between these various "security" and "protection" laws illuminates the many ways that legal liability can be imposed on data activities.

The Draft Law sheds some light on how the government authorities will likely manage different types of data. For example, Article 37 of the Cyber Security Law mentions "critical" and "personal" data without noting which authorities are ultimately responsible for approving cross-border transfers. Read in connection with Articles 7 and 49 of the Draft Law, government agencies at all levels and in different sectors may be empowered to formulate their own guidelines about what constitutes "critical" data, while "personal" data will be subject to the authorities specified in the forthcoming Personal Data Protection Law. Furthermore, the creation of a data security review system (Article 22) will likely result in more guidance on what constitutes national security, which has long been desired by practitioners.

Conclusion

The Draft Law is an important piece of forthcoming legislation that is worthy of continued attention. If the law is passed as most anticipate, we can expect to see more “teeth” during enforcement to punish data security breaches and impose additional controls on data outflow. Although questions regarding implementation remain, we anticipate that the law when passed will be guided by China’s national strategies regarding national security and the digital economy.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your usual Davis Polk contact.

Martin Rogers	+852 2533 3307	**martin.rogers@davispolk.com**
Patrick S. Sinclair	+852 2533 3305	**patrick.sinclair@davispolk.com**
Yuan Zheng	+852 2533 1007	**yuan.zheng@davispolk.com**

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's **privacy notice** for further details.