CHINA'S NEW DATA SECURITY LAW BOLSTERS ITS DATA SECURITY LEGAL REGIME

Date: 9 July 2021

China Data Protection, Privacy, and Security Alert

By: Amigo L. Xie, Xiaotong Wang

On 10 June 2021, the Standing Committee of the National People's Congress of China (NPCSC) approved the enactment of *Data Security Law* (the DSL) of the People's Republic of China (PRC), which will take effect on 1 September 2021. The public was allowed to comment on two drafts of the DSL on 3 July 2020 and 29 April 2021.

Many view the DSL, together with the *PRC Cybersecurity Law* (2017) (the CSL) and the *Personal Information Protection Law (Second Draft)* (the PIPL) as the three pillars that will form China's data privacy and security legal regime, once all take effect.[1]

The DSL will primarily govern the data security of any record of information in electronic or other form (including hardcopies), while the CSL and PIPL focus on network data and personal information, respectively.

Both of the CSL and the DSL are mainly public law. Compared with the CSL, however, the DSL defines data more broadly and is not limited to electronic data from or in the network, which is within the jurisdiction of the CSL. Additionally, the DSL's data protection focus differs from that of the PIPL, which mainly focuses on data privacy from a personal information perspective, whereas the DSL focuses on protecting data that has national or other security implications from a regulatory perspective.

Nonetheless, these three laws have inter-related provisions such as the provisions on critical information infrastructure, important data, local storage requirements, cross-border transfer, etc.

SIGNIFICANCE TO MULTINATIONAL COMPANIES DOING BUSINESS IN OR WITH CHINA

The DSL provides for domestic and extraterritorial jurisdiction. It governs data processing activities, which include the collection, storage, use, processing, transmission, provision and disclosure of data and data security administration within China, and similar activities outside of China that may jeopardize the national security, public interests or the legal rights and interests of Chinese citizens and companies. As a result, multinational companies that have a presence in China or interact with Chinese entities or individuals should take note of this new legislation and its implications.

The underlying purpose of the DSL, among others, is to regulate big internet or high-tech companies that create, collect and process an enormous volume of data (including in electronic form and hardcopies) in China on a daily basis. The law's aim is to control the development of the digital economy in China. As a matter of policy, data is treated as a key production factor and a national security issue by the Chinese government. The DSL will be a fundamental law for China to pursue its data security agenda, as it establishes a comprehensive regulatory framework and provides a legal basis for a variety of ancillary implementing regulations and rules to be issued. It

should be noted that no such regulations or implementing rules have been released under the DSL yet. As with all PRC laws, the DSL provides a general statement of guiding principles. Its implementing regulations, rules and even practice of authorities will provide legal guidance.

KEY HIGHLIGHTS FOR MULTINATIONAL COMPANIES

The DSL could greatly impact multinational companies doing business in or with China, provisions of note deal with the following:

1. Classified and graded data protection system

The DSL lays out a "classified and graded" data protection system that categorizes data into different groups based on its nature and then assigns different levels of importance to the data within each group. The data protection requirements for data in different groups with different importance may vary. This suggests or signals that under the DSL framework, data in different groups or produced across different industries will be regulated differently.

For instance, the *Several Provisions on Automotive Data Security Management* (Draft) was released for public comments on 12 May 2021. This draft has surprised most of the market players in the automobile industry and immediately provoked heated discussions. Among other things, the draft defines the important data in the automotive industry very broadly. According to this definition, even self-driving solution providers and service providers of high definition maps for driving are subject to this draft though they are not typical operators in the automotive industry.

It is expected that some industry-specific rules may follow in the near future.

2. Local storage requirement

The provisions of the DSL that set forth local data storage requirements inter-relate to the CSL's provisions.

Under the CSL, an operator of "critical information infrastructure" in China is required to locally store personal information and important data gathered and produced during its operation within the territory of China. The CSL does not define the "important data" but defines "critical information infrastructure" very broadly.

The DSL affirms this local storage requirement under the CSL and further provides for catalogues for *important data*. Under Article 21 of the DSL, the national data security coordination mechanism shall make overall planning for and coordinate relevant departments of State Council in formulating the important data catalogues and strengthening the protection of important data.

Businesses should monitor important data identified in the catalogues because important data processed by a critical information infrastructure operator in China will be subject to the local storage requirement. Companies handling this type of data will need to implement special protection measures if handling such data to ensure compliance with the laws.

3. Cross-border data transfer

Cross-border data transfers remain a major concern of multinational companies with businesses or employees in China since the CSL took effect in 2017. The DSL and the CSL govern data transfer from China to foreign jurisdictions from different angles.

The CSL previously required an operator of “critical information infrastructure” to go through government-performed security assessments prior to transferring personal information and “important data” overseas. The CSL, itself, is silent on the regulation of cross-border data transfer conducted by other network operators and participants that are not involved in any “critical information infrastructure” operations.

To fill this gap, the DSL provides that any “important data” collected and processed in China is also subject to a security assessment mechanism which will be formulated by the relevant government agencies. Failure to comply with the data transfer rules under the DSL may lead to a fine of up to RMB10 million (approximately US$1.56 million), as well as lead to the revocation or suspension of a company's business license if the non-compliance leads to severe consequences.

The security assessment mechanisms have yet to be laid out under the DSL and the CSL. Two draft bills were proposed in 2017 and 2019 that contained provisions on the security assessment on cross-border transfer of personal information and important data; however, both are still under review by the relevant governmental authorities.

One noteworthy legal quirk involves data related to national security and interests or the performance of international obligations. This data is regulated by the *PRC Export Control Law* (2020) as well. Once so classified, it will have to go through export control formalities and companies may be prohibited by virtue of this law from transferring data so classified overseas.

4. Restriction on cooperation with foreign judicial and law enforcement bodies

The DSL goes further and requires that, without the prior approval of Chinese authorities, any company or individual in China shall not provide any data to foreign judicial bodies or law enforcement bodies. This could potentially affect multinational companies' data submission to the U.S. Securities and Exchange Commission, the Department of Justice, or similar foreign law enforcement bodies or regulators.

The reason specified in the DSL is that such data sharing or transfer requests should be handled by China's relevant authorities in accordance with the provisions of any international treaty or agreement that China has concluded or acceded to, or in line with the principle of equality and reciprocity. Failure to comply with this rule may lead to a fine of up to RMB5 million (approximately US$781,250) if the non-compliance leads to severe consequences.

5. Countermeasures

The DSL states that for any country or region that adopts discriminatory prohibitions, limitations, or other similar measures related to data and the data development and use technology against China in investment, trade and other areas, China may, depending on the actual circumstances, adopt the countermeasures against such country or region.

Obviously, this mainly focuses on restrictions and sanctions imposed by the U.S. against Chinese companies that relate to data and data technology.

OBSERVATIONS

As China continues to build-up its data security legal regime, multinational companies with a presence in China or companies that interact with Chinese individuals or organizations, may find it increasingly challenging to comply with the relevant regulations being promulgated in China in tandem with evolving data security regimes globally.

In addition to understanding and complying with China's new data security legal regime, each multinational company, particularly high-tech companies, should consider auditing their practices in China, as well as developing and executing an aligned global data protection strategy. Companies with a China nexus should also continue to vigilantly monitor new regulations and implementing rules as they are issued in China for the foreseeable future.

FOOTNOTES

[1] The PIPL is still a draft bill under review dated 29 April 2021, but is expected to be officially promulgated very shortly.

KEY CONTACTS

AMIGO L. XIE
PARTNER

HONG KONG
+852.2230.3510
AMIGO.XIE@KLGATES.COM

XIAOTONG WANG
ASSOCIATE

BEIJING
+86.10.5817.6119
XIAOTONG.WANG@KLGATES.COM

K&L Gates is a fully integrated global law firm with lawyers located across five continents. The firm represents leading multinational corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals.