LAW GAZETTE

CHINA LAW, FEATURE - November 2021

Data Protection and Data Security Laws of China

14 min read
by Benjamin Cheong and Yu Peiyi

2021 marks an interesting year for China's data protection scene. On one hand, China reported close to 989 million internet users at the end of 2020. At the same time, 2021 saw the coming into force of two important pieces of legislations concerning data protection and data security in China, namely, the Data Security Law and the Personal Information Protection Law. It has therefore become increasingly important for businesses seeking to tap on the immense Chinese internet market to understand China's data protection regime. This article seeks to examine some of the key features of these new legislations and the changes that they bring to China's data protection and data security landscape and the way MNCs can conduct business in China.

1. Introduction

In February 2021, the China Internet Network Information Centre reported that China had 989 million internet users at the end of 2020. [1] This makes China the country with the most internet users in the world. To give a few indicators, as of December 2020, China had:

- 854 million online payment users,
- 927 million online video viewers, including 873 million short video viewers, and
- 782 million online shoppers. [2]

At the same time, 2021 also marks a significant year for China's data protection scene. In 2021 alone, two key pieces of legislation concerning data protection and data security, the Data Security Law (**DSL**) and the Personal Information Protection Law (**PIPL**), were enacted and will come into force. Together with the Cybersecurity Law (**CSL**) which came into effect earlier on 1 June 2017, they form the core tenets of China's data protection and data security.

It is therefore important for businesses that are seeking to tap on the immense Chinese internet market to have a functional understanding of China's data protection regime, in particular its rules dealing with the protection of Personal Information. This article seeks to examine some of the key features of the PIPL, and the corresponding changes to China's data protection and data security landscape.

2. Legislative History and Purpose

The CSL marks the first of China's three key data protection laws. While the CSL contained provisions relating to the protection of personal information, its primary focus was on "*ensuring network security; safeguard China's cyberspace sovereignty, national security and societal public interest*". [3]

In contrast, the DSL had a more data-protection oriented focus, and seeks to "*regulate data processing activities, protect data security, promote the development and exploitation of data*" [4] . It should also be noted that the DSL's coverage extends beyond Personal Information.

The PIPL was enacted to "*protect rights and interests in Personal Information; regulate activities handling Personal Information; and promote the reasonable use of Personal Information*". [5] It aims to implement Articles 38 and 40 of China's Constitution which enshrined protection for citizens' rights to personal dignity and privacy.

3. Territorial Scope

China's data protection regime under the CSL had no extraterritorial effect. The CSL is applicable to "the establishment, operation, maintenance and usage of networks, as well as network security supervision and management *within the territory of the People's Republic of China (**PRC**)*". [6]

In contrast, with the introduction of the DSL, China's data protection regime gained an extraterritorial bite. The DSL provides that it is applicable to data processing activities within the territory of the PRC, as well as data processing activities *outside the territory of the PRC* that are *harmful* to the national security of the PRC, public interests, or the lawful rights and interests of citizens and organisations. [7]

The territorial scope of China's data protection regime was further expanded by the enactment of the PIPL. The PIPL applies to Personal Information processing activities within the territory of the PRC. In addition, it is also applicable to Personal Information processing activities *outside the territory of the PRC*, if such activities relate to:

i. the provision of goods or services to natural persons within the territory of PRC,
ii. the analysis and evaluation of the actions of natural persons within the territory of the PRC, or
iii. other situations provided for by laws or administrative regulations. [8]

4. How Personal Information is Defined

4.1 Personal Information

Under the CSL, "Personal Information" is defined as "all kinds of information, recorded electronically or through other means, *that taken alone or together with other information, is sufficient to identify a natural person's identity*, including, but not limited to, natural persons' full names, birth dates, identification numbers, personal biometric information, addresses, telephone numbers, and so forth". [9]

Under the PIPL, "Personal Information" is defined as "any type of information *relating to* identified or identifiable natural persons that are stored in electronic or other forms, excluding anonymized information". [10]

While the definition of Personal Information under the CSL and PIPL is phrased differently, except for very limited exceptions, a piece of information that would satisfy the test of Personal Information under one law would in most cases also satisfy the test under the other.

4.2 Sensitive Personal Information

The PIPL introduced the concept of Sensitive Personal Information. "Sensitive Personal Information" refers to Personal Information that can easily lead to the infringement of the personal dignity of natural persons or cause harm to persons or property if leaked or used illegally. Sensitive Personal Information includes biometric information, religious faith, particular identities, medical and health information, financial accounts, location tracking information and personal information of minors under the age of 14.

The processing of Sensitive Personal Information is subject to more stringent requirements which are discussed below. Personal Information processors (**PIPs**) may only process Sensitive Personal Information for specific purposes where fully necessary and must implement strict protective measures when doing so. (Article 28)

5. Processing of Personal Information

5.1 Bases for Processing

The CSL requires Network Operators to only collect, use and disclose Personal Information with the consent of the data subjects. [11] On one hand, this narrows the grounds on which Network Operators may process Personal Information. On the other hand, the processing of Personal Information by persons other than Network Operators are not restricted under the CSL.

The PIPL introduced additional grounds for the processing of Personal Information and is now applicable to all PIPs regardless of whether they are Network Operators. A PIP may process [12] Personal Information so long as one of the recognised bases are met, including situations where:

1. It is necessary for the conclusion or performance of a contract which the individual is a party to;
2. It is necessary for the performance of lawful duties or obligations;
3. It is necessary to respond to public health incidents, or to protect the lives, health and property of natural persons in an emergency; or
4. It is reasonably necessary for news reporting or public opinion oversight in the interest of the public.
5. (Article 13)

Situations where consent is required

Under the PIPL, the PIP is required to obtain the consent of the individual in certain situations, including where:

- the PIP is seeking to engage a Sub-Processor to process Personal Information (Article 23);
- the PIP is seeking to use personal images and personal identifiable information which it has collected in public spaces, for any purposes other than maintaining public security (Article 26);
- the PIP is seeking to process Sensitive Personal Information (Article 29); and
- the PIP is seeking to transfer Personal Information out of the country (Article 39).

5.2 Principles of Processing

The PIPL sets out various principles which PIPs must comply with when processing Personal Information. Such principles include:

- **Legality, legitimacy, necessity, and good faith**. The PIPL provides that Personal Information must be processed in accordance with the principles of legality, legitimacy, necessity, and good faith, and must not be processed through means such as misleading, fraud, or coercion. (Article 5)
- **Necessity / Data Minimisation**. The PIPL provides that the processing of Personal Information must be for a clear and reasonable purpose, relate directly to that purpose, and adopt the method of processing which will have the smallest impact on the individual's rights and interests. Further, PIPs must not collect excessive Personal Information beyond what is necessary for achieving the intended purpose. (Article 6)
- **Openness and Transparency**. The PIPL provides that PIPs must disclose the rules for the processing of Personal Information, including the purpose, method and scope of processing. (Article 7)
- **Accuracy**. The PIPL provides that PIPs must ensure the quality (including accuracy and completeness) of the Personal Information being processed, to avoid adversely impacting an individual's rights and interests. (Article 8)

5.3 Consent

Where Personal Information is being processed on the basis of consent, the PIPL provides that:

- the consent must be provided voluntarily on a fully informed basis (Article 14);
- where there are changes to the purpose of processing, method of processing and type of Personal Information to be processed, fresh consent must be obtained (Article 14);

- the individual must have the right to withdraw his/her consent (Article 15).

PIPs that are processing Personal Information of minors must obtain the consent of their parent or guardian. (Article 31)

Further, PIPs are not allowed to refuse to provide goods or services to an individual on the ground that such individual had not consented to the processing of his/her personal Information or had withdrawn his/her consent, unless the processing of Personal Information is essential for the provision of such goods or services. (Article 16)

5.4 Notification

The PIPL provides that prior to processing any Personal Information, the PIP must inform the individual of the following matters:

1. The name and contact details of the PIP;
2. The purpose and method of processing, the types of Personal Information to be processed, and the retention period;
3. The methods and procedures by which the individual can exercise his/her rights under the PIPL; and
4. Any other matters prescribed by applicable laws or regulations. [13]

In addition, PIPs that are seeking to process Sensitive Personal Information must also inform the individual of the necessity of such processing and the impact of such processing on such individual's rights and interests. (Article 30)

5.5 Retention of Personal Information

The PIPL provides that Personal Information must not be retained beyond what is necessary for achieving the purpose of processing, unless otherwise provided by applicable laws or regulations. (Article 19)

5.6 Engagement of Sub-Processors

Under the PIPL, where PIPs engage another processor (**Sub-Processor**) for the processing of Personal Information (**Sub-Processing**), they must enter into an agreement with the Sub-Processor. (Article 21)

The PIPL further provides that PIPs that seek to engage Sub-Processors must notify the individuals and obtain the individual's consent. (Article 23)

Sub-Processors must take necessary measures to protect the Personal Information that they are Sub-Processing in accordance with the PIPL and other applicable laws and applications, and assist PIPs in complying with their obligations under the PIPL. (Article 59)

5.7 Consumer Protection

In recent years, some e-commerce platforms have profiled their existing customers and conducted data analytics on such customers to derive insights on their spending habits, spending power, personal preferences, and price sensitivities. Such platforms are then able to charge the Customers higher prices for the same goods and services, with the knowledge that such prices would still be acceptable to the customers. Such practices allow platforms to profit at the expense of the consumers. [14]

Article 24 of the PIPL is precisely targeted at curbing such discriminatory practices. Article 24 of the PIPL requires PIPs that are using Personal Information for automated decision making to ensure that the decision-making process is transparent, the results are fair and equitable, and not unreasonably discriminate against individuals on trading terms (such as prices).

6. Cross Border Transfer of Data

6.1 Requirements for Cross Border Transfer

China adopts a differentiated approach to the cross-border transfer of Personal Information, which hinges on the type of entity concerned and the volume of Personal Information that such transferor is processing.

The concept of data localisation was first introduced into the Chinese data protection regime by the CSL, which required CIIOs to store within the territory of the PRC the Person Information and important data that they have collected or generated in carrying out operations in PRC.

The enactment of DSL and PIPL now makes clear that while certain common requirements will apply to all entities that are seeking to transfer Personal Information outside the PRC, there are also different specific requirements that may apply, depending on the nature of the transferor concerned and the volume of Personal Information that such transferor is processing. This is represented in the table below:

Type of Entity	Specific Requirements	Common Requirements
Critical Information Infrastructure Operators (**CIIOs**)	• Personal Information and important information collected or generated in the PRC must be stored within the territory of the PRC. • Must pass a security assessment administered by the CAC if it is necessary for	• Take the necessary measures to ensure that the Personal Information processing activities carried out by the foreign recipients will accord a standard of protection for the transferred Personal Information equivalent to that imposed under the PIPL. [16] • Inform the relevant individual of the name and contact details of the foreign recipient, processing purpose, processing method, types of

Type of Entity	Specific Requirements	Common Requirements
PIPs that are processing Personal Information above a certain threshold as determined by the Cyberspace Administration of China (**CAC**) (**Designated PIPs**)	such entities to transfer Personal Information out of the territory of the PRC. [15]	Personal Information and the methods and procedures by which the individual can exercise his/her rights under the PIPL, and obtain such individual's consent. [17] • Conduct a Personal Information Protection Impact Assessment (**PIPIA**) prior to the transfer. [18]
Other PIPs	• Must fulfil at least one of the following requirements: 1. passing a security assessment administered by the CAC; 2. undergoing a Personal Information protection accreditation conducted by professional organisations in accordance with the conditions prescribed by the CAC; 3. entering into a contract with the foreign recipient of Personal Information in accordance with the standard contractual terms issued by the CAC which sets out the parties' rights and obligations; or 4. compliance with other applicable laws, regulations or the CAC. [19]	

It should be noted that the threshold for "Designated PIP" is not expressly set out under the PIPL. However, it appears that once said threshold is reached or exceeded, the default expectation for such PIP to store Personal Information that they are collecting or processing within the PRC would be triggered. As such, businesses that are collecting or processing a large volume of Personal Information in the PRC should monitor developments in this area closely.

6.2 Restrictions on Cross Border Transfer

The cross-border transfer of Personal Information out of the PRC may be restricted in the following situations:

- **Where the transfer is pursuant to a request by foreign judicial or law enforcement agencies.** Article 41 of the PIPL provides that PIPs must not provide Personal Information that is stored within the PRC to foreign judicial or law enforcement agencies of its own accord without the permission of the competent state organs of the PRC. A similar requirement is also found under Article 36 of the DSL.

> "
> It should be noted that Article 41 of the PIPL applies to all Personal Information that is stored within the PRC, and is not only confined to the Personal Information of PRC citizens. This may pose a significant compliance issue for organisations that store Personal Information within the PRC, if they are also subject to legal obligations to disclose Personal Information to judicial or law enforcement agencies in their own jurisdictions.

- **Where the recipient is Blacklisted.** Article 42 of the PIPL provides that where organisations or individuals outside the territory of the PRC carry out Personal Information processing activities that are harmful to the rights and interests of PRC citizens, or threaten the PRC's national security or public interests, the CAC may place such organisations or individuals on a list which restricts or prohibits the transfer of Personal Information to such organisations or individuals (**Blacklist**), publish such Blacklists, and employ measures to restrict or prohibit the transfer of Personal Information to such blacklisted organisations or individuals.
- **Where the recipient jurisdiction adopts discriminatory prohibitions or restrictions against the PRC.** Article 43 of the PIPL further provides that where any country or region adopts discriminatory prohibitions, restrictions, or other similar measures against the PRC in terms of Personal Information protection, the PRC may employ equal measures against that country or region based on the circumstances.A similar reciprocal restriction is also found under Article 26 of the DSL, which provides that where any country or region adopts discriminatory prohibitions, restrictions, or other similar measures against the PRC in terms of investment, trade or other matters relating to data or technology relating to data use and exploitation, the PRC may employ equal measures against that country or region based on the circumstances.Organisations should therefore be sensitive to restrictions imposed on the transfer of Personal Information into the PRC by other countries, and note that this might trigger a reciprocal restriction by the PRC against recipients in such countries.

7. Rights of Data Subjects

The PIPL recognizes various rights of individuals in relation to his/her Personal Information, including:

- Right to withdraw consent. (Article 15)
- Right to object to automated decision making. (Article 24)
- Right to information. (Article 44)
- Right to restrict or reject the processing of Personal Information. (Article 44)
- Right to access and make copies of his/her Personal Information. (Article 45)
- Right to data portability. (Article 45)
- Right to correction or amendment of Personal Information where the Personal Information is inaccurate or incomplete. (Article 46)
- Right to request deletion of Personal Information. (Article 47)
- Right to the explanation of the rules of Personal Information processing. (Article 48)

Article 50 of the PIPL requires PIPs to establish a *convenient* mechanism for accepting and addressing requests from individuals to exercise their rights. A PIP is required to provide an explanation to an individual if it refuses to accede to an individual's request to exercise his or her rights. An individual may commence legal proceedings against a PIP if it refuses to accede to such individuals' request to exercise his or her lawful rights.

8. Obligations of PIPs

8.1 Taking Measures to Ensure Compliance and Protection

The PIPL provides that PIPs and must employ necessary measures to ensure the security of Personal Information that they process. (Article 9)

The obligation to protect Personal Information is further detailed by Article 51 of the PIPL, which requires PIPs to adopt measures to ensure the Personal Information processing activities comply with applicable laws and regulations, and prevent unauthorised access, leaking, alteration and loss of Personal Information. Such measures include:

1. Formulate internal security management systems and operating procedures;
2. Categorise and manage Personal Information based on their categories;
3. Employ technical security measures such as encryption and de-identification of Personal Information;
4. Impose access restrictions on individuals appointed to process Personal Information;
5. Conduct security education and training for employees periodically;
6. Formulate and implement Personal Information security incident response plans; and
7. Any other measures required by applicable laws and regulations.

8.2 Appointment of DPOs and representatives

The PIPL provides that Designated PIPs must appoint a person in charge of Personal Information protection (**DPO**) who shall be responsible for overseeing Personal Information processing activities and implementation of protective measures. (Article 52)

The PIPL further provides that where PIPs are processing Personal Information outside the PRC, for the purpose of analysing or evaluating the actions of natural persons within the territory of the PRC, such PIPs must establish a special institution or appoint representatives *within the PRC* for handling matters relating to the protection of Personal Information, and notify the name, contact details of such institution or representative to the relevant authorities. (Article 53)

8.3 Conducting Personal Information Protection Impact Assessment

The PIPL provides that PIPs must conduct a PIPIA prior to, and maintain processing records when carrying out any of the following actions:

1. processing Sensitive Personal Information;
2. conducting automated decision making using Personal Information;
3. engaging Sub-Processors or providing Personal Information to other PIPs;
4. disclosing Personal Information;
5. transferring Personal Information out of the country; and
6. processing Personal Information in any other way which has a significant impact on the rights and interests of the individual. [20]

The PIPL further provides that PIPIA must address the following issues:

1. whether the purpose of processing Personal Information are lawful, legitimate and necessary;
2. the impact on the rights and interests of the individual, and security risks;
3. whether the protective measures taken are lawful, effective and commensurate to the level of risks. [21]

The PIPIA and processing records must be retained for at least three years.

8.4 Data Breach Notification

Where the leak, alteration or loss of Personal Information (**Data Breach**) has occurred or might have occurred, PIPs are required to adopt remedial actions immediately, and notify the PIPD and affected individuals. (Article 57)

8.5 Important Internet Service Providers

Article 58 of the PIPL provides that PIPs that (a) provide important internet platform services, (b) have a larger number of users, or (c) operate under complex operational models (collectively **Important Internet Service Providers** or **IISPs**) must:

1. establish Personal Information protection compliance system and establish an independent body comprising primarily of external members to supervise the state of Personal Information protection;
2. comply with principles of openness, fairness, and equity when drafting platform rules, and make clear its standards for processing Personal Information and protection of Personal Information by providers of goods or services on the platform;
3. stop providing services to providers of goods or services on the platform that process Personal Information in serious violation of laws and administrative regulations; and
4. periodically publish social responsibility reports on the protection of Personal Information, and accept societal supervision.

It is worth noting that the concept of IISP is only mentioned once in the PIPL, and the interplay between IISPs and Designated PIPs are unclear at the present. The PIPL also does not provide further clarifications on what constitutes "important internet platform services", "a large number of users", or "complex operational models", although the reference to "providers of goods or services" would suggest that many of the renowned large internet platform players (particular those that sustain an entire ecosystem) may be caught under this provision. It is expected that these issues will be clarified by further subsidiary legislation to be released in the future.

With that being said, it is at least clear that under the PIPL framework, not only are PIPs and individuals for ensuring compliance with the PIPL, large internet platform players also have an obligation to ensure that members of its network are compliant.

9. Enforcement

Where Personal Information is processed in violation of the PIPL, or where Personal Information is processed without adherence to the Personal Information protection obligations stipulated under the PIPL, the penalties that may be imposed against the PIPL include:

- Orders for rectification;

- Issuance of an order for suspension or cessation of service; and
- Imposition of financial penalties against the PIP, the DPO or other directly liable individuals.

The penalties under the PIPL are similar to the penalties imposed against network operators and internet goods or service providers under the CSL, [22] and those imposed against organisations or individuals carrying out data processing activities in breach of the DSL. [23] However, the maximum quantum of financial penalties that may be imposed under the PIPL is the highest amongst the trio.

10. Conclusion

The enactment and coming into force of the DSL and PIPL brings about important ramifications for both businesses operating in China as well as businesses outside China that fall within their scope. It is therefore necessary for businesses to carefully re-examine their business models, rethink their data strategies, and re-evaluate their value propositions in light of the DSL and PIPL, to ensure that they can operate sustainably and in compliance with the applicable laws involved.

Endnotes

1	http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/202102/t20210203_71361.htm
2	http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/202102/t20210203_71361.htm
3	CSL, Article 1
4	DSL, Article 1
5	PIPL, Article 1
6	CSL, Article 2
7	DSL, Article 2
8	PIPL, Article 3
9	CSL, Article 76
10	PIPL, Article 4
11	CSL, Article 22, 41, 42
12	Processing of Personal Information includes the collection, storage, use, processing, transmission, provision, publication, and erasure of personal information. PIPL, Article 4
13	PIPL, Article 17
14	http://www.xinhuanet.com/fortune/2021-06/07/c_1127539823.htm
15	CSL, Article 37, DSL, Article 31, PIPL, Article 40
16	PIPL, Article 38
17	PIPL, Article 39
18	PIPL, Article 55
19	PIPL, Article 38
20	PIPL, Article 38
21	PIPL, Article 39
22	CSL, Article 44, 64
23	DSL, Article 45

Tags: CHINA, CYBERSECURITY, DATA PROTECTION, DATA SECURITY, PERSONAL INFORMATION PROTECTION

Benjamin Cheong
Partner
Technology, Media & Telecommunications Practice Group
Rajah & Tann Singapore LLP
E-mail: benjamin.cheong@rajahtann.com

Benjamin is a partner in Rajah & Tann's Technology, Media and Telecommunications practice group. He has practised in Singapore, Hong Kong and Shanghai (as a foreign lawyer), and has been involved in many complex cross-border and multi-jurisdictional deals across Asia.

Benjamin has more than a decade of experience in advising clients on contentious and non-contentious matters, with a particular focus on commercial intellectual property, technology and franchising/licensing transactions, technology outsourcing deals and data protection compliance. He has worked on a number of cross-border joint venture and mergers and acquisition deals across Asia, with a particular focus on the PRC. With the growth of the digital and knowledge-based economy, Benjamin has a keen interest in cybersecurity, blockchain technology, fintech, insurtech, medtech, digital payments and AI and keeps abreast with developments in these new technologies and industries.

Yu Peiyi
Associate
Technology, Media & Telecommunications Practice Group
Rajah & Tann Singapore LLP
E-mail: peiyi.yu@rajahtann.com

Peiyi is an associate in Rajah & Tann's Technology, Media and Telecommunications practice group. He works on a portfolio of Chinese technology companies and regularly advises clients on various intellectual property, data protection, cybersecurity, content regulation, advertising, and general corporate and commercial matters. He also takes a keen interest in legal and political developments in China and ASEAN, and is a member of various organisations that are aimed at raising youth awareness and understanding of China-ASEAN relations, including Business China Youth Chapter and The Young SEAkers.

Peiyi is also one of Singapore's first 'Hybrid Lawyer' with a career in both the Legal and the LegalTech industry. As a Legal Technology Consultant in Rajah & Tann Technologies, he works on e-discovery projects, implementing contract automation and contract lifecycle management solutions, and developing e-learning content.