VOL.5 ISSUE 3
DROIT PENALE: INDIAN LAW JOURNAL ON CRIME & CRIMINOLOGY
ISSN: 2456-7280

DATA PROTECTION LAW IN CHINA

Krish Bhatia[1]

Abstract

In layman's terms, the word " Privacy " means keeping personal info and matters secret or inside oneself. In broad terms, 'Privacy' means to have management over one's info, its method, and mode of assortment, and keeping it free from interference and intrusion. Earlier 'Privacy' was commonly utilized in philosophical, political, and in legal discussions. The thought of privacy was coined by Aristotle. He distinguished it into public and private spheres that were associated with political activities, family, and domestic life severally.

The word "Data protection" refers to the practices, safeguards, and binding rules place in place to shield your info and confirm that you simply stay on top of things of it. protective knowledge from compromise and ensuring knowledge privacy square measure different key elements of data protection; but, wherever there are not any laws to enforce within the event of a breach, the price of those rights are lost. to uphold the standard of these rights, sovereign nations of the earth place in place laws and different mechanisms to make sure them.

These all things are also called "PERSONALLY IDENTIFIABLE INFORMATION" (PII)

Governments even have an interest in ensuring the protection of personal knowledge. In 2015, criminals scarf twenty one.5 million records from the USA workplace of Personnel Management that contained the sensitive personal knowledge of federal workers and their members of the family. this type of attack is happening tons of oft across the planet, and countries should take action to raised shield individuals' info.[2]

keywords: Personal information protection law (PIPL), PERSONALLY IDENTIFIABLE INFORMATION" (PII), DATA SECURITY LAW (DSL), General Data Protection Regulation (GDPR)

PERSONAL INFORMATIONAL PROTECTION LAW

China has passed a private data protection law, law, called the Private Information Protection Law (PIPL), which is about to require effect on All Saints' Day.

It was proposed last year signaling an intent by China's communist leaders to clamp down on unscrupulous data collection within the commercial sphere by putting legal restrictions on user data collection. China unveiled its draft of the private Information Protection Law for public consultation on Oct. 21, 2020. Taking a better check out the draft PIPL, it's easy to ascertain many provisions in it are inspired by the EU General Data Protection Regulation. The draft

[1] 3rd Year Law Student pursuing BALLB from Chandigarh University.
[2] Privacy https://en.wikipedia.org/wiki/Privacy

PIPL, which contains 70 articles and hefty fines, once it comes into force, is going to be China's first comprehensive law on the protection of private data. little question it'll bring significant impact to companies with operations in China or targeting China as a market despite no business presence in China.

The draft PIPL applies to the processing of individuals' data that takes place in China no matter the nationality of such individuals. Unlike the PRC Cyber Security Law, which provides limited extraterritorial application, the draft PIPL proposes clear and specific extraterritorial application to overseas entities and individuals that process the private data of knowledge subjects in China

(1) for provision of products and/or services to data subjects in China

(2) for analyzing or assessing the behavior of knowledge subjects in China

(3) in other circumstances as provided by Chinese laws and regulations.

Considering certain resemblance of this provision to Article 3(2) of the GDPR, it might not be a surprise going forward if Chinese regulators consider the regulatory approach as illustrated within the European Data Protection Board "Guidelines 1/2018 on Territorial Scope."

The draft PIPL also specifically provides various data protection principles, including transparency, fairness, purpose limitation, data minimization, limited retention, data accuracy, and accountability.

The definition of "personal data" and "processing" under the draft PIPL is nearly as broad as its equivalent term under the GDPR. Organizations or individuals outside China that fall under the scope of the draft PIPL will get to found out a fanatical organization or appoint a representative in China and also report relevant information of their domestic organization or representative to Chinese regulators.

The PIPL represents one pillar of China's emerging data protection architecture that has a myriad of other laws, industry-specific regulations, and standards. as an example, the recently enacted DSL sets forth a comprehensive list of requirements regarding the safety and transferability of other sorts of data. It also establishes a "marketplace for data" to enable data exchange and digitalization. Additionally, the PIPL explicitly references China's Constitution to supply a more firm legal basis for the implementation of its data protection goals (Art. 1). As such, the PIPL shouldn't be viewed in isolation but rather examined concerning these other regulatory tools that serve complimentary, albeit different purposes.

The PIPL will mainly function China's comprehensive data protection law, following during this respect the ECU approach which clearly distinguishes the protection of privacy from the protection of people concerning the processing of their personal information ("data protection"). Its officially declared aims are thus:

• to protect the rights and interests of people

• to regulate personal information science activities

• to safeguard the lawful and "orderly flow" of knowledge [3]

• to facilitate reasonable use of private information

ENFORCEMENT

The law doesn't create an independent authority dedicated to data protection enforcement. The Cyberspace Administration of China (CAC) is that the primary body liable for data protection enforcement, but several other regulators can also administer the law.

In addition, the Chinese government may delegate further responsibility to a Technical Committee (e.g., TC260) to develop standards to clarify the meaning of the law and supply more guidance on enforcement.

The PIPL stipulates penalties for violations and non-compliance, including the suspension or termination of application programs unlawfully handling data. Non-compliance not only involves unlawfully processing personal information but also includes failing to adopt proper necessary security protection measures following further regulations.

The law makes a distinction between two sorts of violations. within the first instance, the departments fulfilling data protection duties will order a correction, confiscate unlawful income, and issue a warning.

• If the info handler refuses to correct the violation, it'll receive a fine of less than 1 million RMB ($150,000).

• Persons who are directly responsible and responsible can also receive a fine between 10,000 and 100,000 RMB ($1500–$15,000) (Art. 66).

[3] https://www.dataversity.net/careful-derived-data/#:~:text=Derived%20data%20is%20data%20that,is%20repeatedly%20deposited%20and%20withdrawn

• In serious violations, the fine could also be increased up to 50 million RMB ($7,500,000) or 5% of annual revenue for the prior financial year (Art. 66). The law doesn't specify whether annual revenue is going to be calculated to support global turnover.

Acts deemed illegal under PIPL are going to be recorded and made public within the social system (Art. 67).

In addition, the PIPL stipulates that engaging in personal information handling activities that harm national security or the general public interest also constitute violations (Art. 10) but no specific penalty is provided for such harms. Violations of the law are going to be publicly recorded and will cause removal from serving as a director, supervisor, or senior manager of the relevant enterprise for a period of your time.

Importantly, the PIPL provides a mechanism for people to receive compensation from data handlers through judicial redress for the loss (damage) they suffered or the benefit the handler obtains "if the processing of private information infringes upon the rights and interests of the individuals" (Art. 69). If it's difficult to work out compensatory damages or the advantages unlawfully obtained, a People's Court may take under consideration the relevant circumstances and render an appropriate award. The second version of the draft PIPL has reversed the burden of proof for the parties during a tort action against PI infringement so that data handlers that can't prove they're not guilty of the harm suffered are going to be liable. Additionally, when data handlers refuse an individual's request to exercise data rights, that individual may file a lawsuit during a public court (Art. 50).

Finally, when a violation of the law infringes on the rights and interests of the many individuals, the People's Procuratorates, and therefore the relevant enforcing agencies and departments may file a lawsuit with a People's Court. One such example concerns the Civil Public Interest Litigation mechanism, which effectively operates as civil prosecution of large-scale violators of the law.

The DSL lists multiple government authorities which will oversee data security matters: • On the central government level, the Central National Security Leadership Organ1 is liable for issuing and overseeing national data security strategies and major policies and is required to determine national data security working and coordination mechanism (Mechanism). National security and peace bureaus are liable for data security supervision and management within their respective remits. • On the regional and departmental levels, local governments and regulatory authorities are liable for data security in their respective regions and industries In parallel, the Cyberspace Administration of China is liable for coordinating, overseeing, and supervising network data security. The DSL requires industrial organizations to issue data security codes of conduct and organizational standards, and guide members to strengthen the protection of knowledge security. additionally, the DSL entitles individuals and entities to report activities in violation of the DSL to related authorities and requires the authorities to affect the reports on time and maintain the confidentiality of the reports and therefore the reporters' information.

DEVELOPMENT of LAW

In January, the government-backed China Consumers Association had accused internet companies of violating customers' rights by misusing personal data and "bullying" people into

purchases and promotions. "Consumers are being squeezed by data algorithms and becoming the targets of technical bullying," the association had said.

"Companies must stop using systems to scan through consumers' personal data and offer them different prices for goods supported that information," it had added.

Following this, China's market regulator had also slapped fines on Tencent and asked it and its affiliated companies to relinquish exclusive rights to music labels. China's State [4]Administration for Market Regulation, during a statement, had said, "To restore market competition, Tencent and its affiliated companies must end their exclusive music copyrights within 30 days and stop charging high prepayment and other copyright fees."

However, Chinese companies' use of knowledge had come to the fore only Beijing's cyber security agency launched a search into ride-hailing group Didi Chuxing days after it raised quite $4 billion during an initial public offering in June.

The Cyberspace Administration of China had asked Didi to prevent accepting new user registrations saying that the app "has serious violations of laws and regulations concerning the gathering of private information". Tens of thousands of consumers had complained about having to pay more for hailing a taxi using an iPhone than a less expensive mobile model or for tickets if they're profiled as a traveler, China's consumer protection watchdog had said.

1. Legal Sources for private Data Protection

There has already been a basic system established for shielding personal data, which sets out the compliance requirements for market players to follow. This system consists of laws, administrative regulations, department regulations/provisions by national regulatory bodies, statutory national standards, national standards recommended for application also as industry standards, etc. The author hereby summarizes or refers to certain key provisions about data protection as follows:

• Article 25 of National Security Law of the People's Republic of China

= It specifies that the state shall establish a network and knowledge security safeguards systems; the state shall safeguard the safety of data systems and data for critical information infrastructure ("CII") and key sectors; the state shall prevent, stop and penalize cyber-related crimes like network attacks, intrusion, theft also as spreading illegal and harmful information, etc.

• Article 111 of General Provisions of the Civil Law of the People's Republic of China

= It sets out the essential principle that a natural person's data shall be protected by law; any organization and individuals must collect personal data after obtaining the private data subject's

[4] https://academic.oup.com/grurint/article/69/12/1191/5909207#220134885

consent and conduct the gathering consistent with the law; they shall make sure the security of the private data collected; illegal collection, using, processing and transmitting of others' data, illegal transaction of selling / purchasing personal data, disclosure of private data shall be prohibited.

The Cybersecurity Law sets out the legal principles and high-level requirements on the protection of private data collected. The compliance requirements began by this law universally apply to all or any network operators. Certain provisions thereof are almost like those contained in European Union's GDPR...

Provisions on the Cyber Protection of Children's Personal Data, which are administrative regulations dedicated to strengthening the protection of children's data collected or processed via networks within China. These provisions began more detailed and stringent compliance requirements as compared with those began by the Cybersecurity Law.

2. Personal Data Protection Concepts

Personal data: There are slightly different definitions for this terminology. consistent with the Cybersecurity Law, personal data refers to varied information which is recorded in electronic or other forms and used alone or together with other information to acknowledge the identity of a natural person, including but not limited to call, date of birth, ID number, personal biological identification information (biometric data), address and phone number of an equivalent.

However, for lawful prosecution and trial of the suspected crime of infringing citizen's data, the Interpretation on Criminal Cases of Infringing on Citizen's Personal Data expands the definition of "personal data" to incorporate various information, which, solely or during a combination of other information, reflects the activities status of specific natural persons, including telecommunication contact information, account passwords, property status, whereabouts and tracking record, etc. The national standards recommended for application, i.e., "Information Security Technology - Personal Data Security Specification" adopts an equivalent expanded definition.

Sensitive personal data: The laws and regulations fail to define what sensitive personal data refers to. However, consistent with the private Data Protection Specification, it refers to the private data which can probably cause personal and property damage, or is sort of possible to end in reputation damage, physical or psychological state damage or trigger discrimination treatment to the private data subject, should such data be disclosed, illegally provided or misused.

Persona data subject: consistent with the private Data Security Specification, it refers to the natural person identified by personal data.

Controller: Personal Data Security Specification defines the controller as organizations or personals who shall have the proper to work out the aim of processing and the way such data is processed, etc.

Joint controller: Personal Data Security Specification doesn't define this terminology. However, the currently applicable version of private Data Security Specification lists samples of joint controllers. Taking as an example, service platforms and therefore the contracting

business owners on these platforms constitute joint controllers. Where the controller and therefore the third party constitute joint controllers, the controller shall, alongside the third party, determine the info security requirements to be satisfied and identify respective security-related responsibilities and obligations byways of signing contracts with the third party, etc. Provisions of identification of responsibilities and obligations by and amongst joint controllers by way of agreements, etc also are included within the Revised Version of private Data Security Specification.

3. Territorial Scope of Chinese Personal Data Protection Legislations

In general, the currently effective data protection legislation has no extraterritorial effect. Taking as an example, the cornerstone data protection related law, the Cybersecurity Law, provides that it applies to construction, operation, maintenance, and use of networks also as supervision and administration over cybersecurity within China's territory.[5]

However, please note that the Measures for Security Assessment of Cross-border Transfer of private Data, require the overseas entities collecting personal data within China's territory via the web, etc during its operational activities shall, through the appointment of the personal representative or organizations, perform the responsibilities and obligations of network operators defined therein. The foregoing requirement extends the territorial scope of application to overseas entities collecting personal data from China. To a particular extent, it's almost like GDPR provisions that non-EEA entities providing services or goods to EU residents or monitoring activities of EU residents shall be subject to the regulation by GDPR.

Entities engaging within the collection of private data within China via networks are recommended to stay alert on the legal updates during this regard.

4. Processing Principles

The following are the summarized major principles for processing personal data consistent with the Cybersecurity Law:

Lawfulness : The collection/use/processing of private data shall not violate the laws, administrative regulations or the agreement concluded with the private data subjects.

Transparency: Network operators must publish rules for collecting and using personal data and inform the private data subjects of the purpose(s) and scope that the info is collected/used. The methods during which the info is collected/used must even be notified.

Consent: Consent must be obtained from personal data subjects before the collection/use of their data. The Cybersecurity Law doesn't list specific situations where such consent isn't required. Certain sector-specific laws / administrative regulations grant relevant regulatory

[5] https://www.zdnet.com/article/chinas-personal-data-protection-law-kicks-in-today/

bodies / authorized entities the facility to collect/use personal data without the consent of the people concerned. Moreover, the private Data Protection Specification specifies that no consent is required surely specific circumstances, including but not limited to those concerning national security, peace, criminal investigation/prosecution/enforcement of sentences, etc, or those situations for shielding significant rights and interests of private data subjects or others. the private Data Protection Specification also requires obtaining explicit consent from personal data subjects in terms of sensitive personal data.

Purpose limitation: the private data subjects must be told of the purpose(s) of collecting/using personal data by network operators. consistent with the private Data Protection Specification, the utilization of private data shall not exceed the scope which is directly or reasonably concerning the aim notified by the controller before collecting the info, and where it's required to exceed the scope, further explicit consent must be obtained from the private data subjects.

Data minimization: consistent with Article 41 of the Cybersecurity Law, network operators shall adhere to the principle of "necessary" when collecting and using personal data and shall not collect personal data irrelevant to their service provided to non-public data subjects. Guidelines and draft national standards for identifying situations of excessive collection of knowledge were formulated or released for comments.

Integrity and confidentiality: Network operators must take technical measures and other measures to make sure the safety of private data, including protection against leak, destruction, or damage. Personal data shall not be provided to other parties without the consent of the info subjects or statutory requirements unless the info has been processed in a way that it can not identify the precise data subjects and can't be restored to the status enabling identification of specific data subjects.

Storage limitation: this will be inferred from the principle of "necessary" consistent with the Cybersecurity Law. the private Data Protection Specification further defines the time frame for storing the private data, which shall be limited to the minimum periods required for realizing the purpose(s), and therefore the data shall be properly disposed of by deletion.

5. Personal Data Subjects' Rights

The Cybersecurity Law provides for the subsequent data subjects' rights:

Right to information: Before the collection/use of private data by the network operators, personal data subjects shall have the proper to be notified of the aim of collection/use of the private data, the way of collection/use, and therefore the scope of private data to be collected/used.

Right to deletion: Personal data subjects shall have the proper to request deletion of their data if they discover network operators' collection or use of the info violates compliance requirements.

Right to rectification: Personal data subjects who discover their data collected or stored is wrong shall have the proper to request rectification by network operators.

6. Security of private Data

The Cybersecurity Law sets out the network operators' obligations to make sure cybersecurity, which is that the basis for ensuring the safety of data, including personal data. One general requirement is to implement the graded system for cybersecurity protection, which isn't a replacement requirement for network operators.

Such a graded system requires the implementation of technical safeguard measures in respect of physical security, network security, host security, applications security, and data security. It also requires the implementation of organizational safeguard measures covering the formulation of internal security rules/regulations and processes, the establishment of knowledge protection department/data protection positions, construction/maintenance etc.

7. Localization and International Transfer of private Data

The following mainly summarizes the wants on the place of storing and international transfer of private data collected and generated by CII network operators.[6]

Localization

Important data and private data collected and generated during the domestic operations of operators of CII shall be stored within China's territory consistent with the Cybersecurity Law.

The Cybersecurity Law provides a non-exhaustive list of industries and sectors of which the network facilities and knowledge systems fall within the CII category, like public communications, information services, energy, transport, water conservancy, finance, public services, and e-government, etc. The law also vests the State Council the facility to develop regulations over the precise scope of CII and therefore the security measures required for CII.

Please note that the Regulations for the safety Protection of Critical Information Infrastructure expands CII scope to incorporate network facilities and knowledge systems operated/administered by government agencies and entities from the subsequent sectors: education, social welfare, environmental protection, public utilities, broadcasting television networks, cloud computing, big data, etc. Those scientific and research entities from sectors of national defense, large equipment manufacturing, chemicals, food, and drug, etc also are included.

References

1. China's personal data protection law kicks in today
2. A look at China draft of personal information protection law
3. Explained: China’s new data privacy laws and its impact on the tech industry
4. New privacy laws will soon take effect in China

[6] https://thediplomat.com/2021/08/chinas-personal-information-protection-law-and-its-global-impact/