Data Protection in China

Jennifer Feng, lawyer in Guangzhou

December 2021

With the rapid development of information technology, more and more service or products providers collect, store, process, analyze and/or use all kinds of data to find business opportunities. Through big data technology, these providers can easily learn our name, gender, address, hobbies, or even our family information, income level, health status, etc. In pursuit of profits, some companies began to improperly collect, process, or resell people's personal information, even violate the privacy of individuals.

The big-data mining and personal information resale have opened the door for criminals, especially fraudsters. Those companies that have acquired the personal data of millions or even billions of individuals actually gain super power. They are able to easily manipulate people's behavior. For example, a UK data consultancy firm, Cambridge Analytica, was alleged that it misused the data of millions of Facebook users for Donald Trump's presidential campaign in 2016. Thus, the PRC government is more and more concerned about the misuse of big data.

On the other hand, the rapid development of information technology is leading our life and society to be more efficient and transparent. In today's China, people rarely use cash in their daily life, in contrast, they finish their payment via the app WeChat and/or AliPay on their mobile phone. In recent years, the majority of buying and selling activities happen online. The extensive use of e-application system and biometric identification enable people to deal with things at home by just clicking buttons on their phones, which cut short the application time from months or days to minutes. Pre-setting the nationwide e-application systems also makes the application procedure more predictable and transparent.

Thus, it becomes a big issue for the PRC government to balance the benefit and negative impact of big data technology. In this article, we will try to give our readers an overview of laws and regulations related to data protection in China.

For data security, China's legislation has been enacted separately in the areas of civil, criminal and administrative Law.

Civil Law System

Civil law mainly deals with the relationship between natural persons, or the relationship between a natural person and a legal person. Therefore, the main

concern under the civil law system is the protection of personal information. Before the popularity of information technology, China's civil law legislation related to data protection mainly focused on personal rights such as life, health, portrait, privacy, reputation, etc. An individual whose rights is infringed could seek judicial relief under *General Principles of Civil Law* (The predecessor of the Civil Code), and *Tort Liability Law*, which is a secondary legislation of civil law.

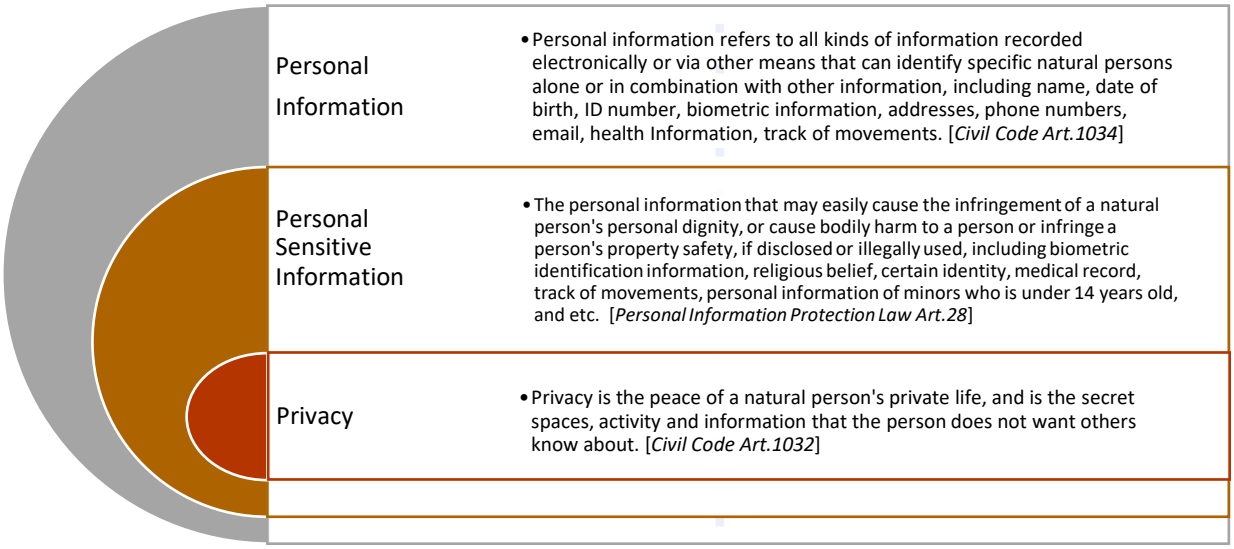
After entering the information era, some personal information that didn't seem important before, such as name, address, email, track of a person's movement, if combined with other information, may be used to deduce the valuable or private information of a person, e.g., a person's consumption habits, hobbies, interpersonal relationship. Thus, a more specific and comprehensive secondary law was introduced, i.e. *Personal Information Protection Law* (Effective on November 1, 2021).

Under the civil law system, personal information is classified as three levels according to their importance and sensitivity. Please refer to the chart below.

Personal Information Protection Law mainly stipulates the rules of processing personal information and sensitive personal information, the rights and obligations of individuals in the processing of personal information. The law also provides guidelines on handling the personal information by state organs, as well as rules for cross-border transmission of personal information.

According to the law, processing of personal information includes collection, storage, use, transmission, providing, publicizing, deletion, etc. The activities involving in processing personal information of natural persons within the border of China are also subject to this law, such as the activities aimed to provide product or service to domestic people, analyze and evaluate the behavior of natural persons in China, or other stipulated situation.
The law stipulates four basic principles for natural person's data processing:

- Lawfulness: Any organization or individual must not illegally collect, use, process or transmit other person's personal information. It is prohibited to illegally trade, provide or publicize personal information.



It is prohibited to process personal information that may cause harm to national security or public benefit. The processers are obliged to take the necessary measures to ensure safety of personal information.

- Justification: This principle requires that the purpose of processing personal information must be specific, clear, and reasonable. The processors shall follow the principle of openness and transparency. They are required to disclose their rules of processing personal information, and express the purposes, methods, and scope of processing.

- Necessity: The collection of personal information should be limited to the minimum extent for fulfilment of the process purpose.

- Good Faith: Any organization or individual shall obtain informed consent from natural persons before they process personal information except several stipulated situations (Emergency Avoidance). Misleading, intentional omission or obscure language may cause the consent being void. The processing shall not exceed the scope of consent.

Processing sensitive personal data is prohibited unless a personal data processor aims to a specific purpose with sufficient necessity and takes strict protective measures. In addition, the individual's informed consent shall be obtained in advance unless the law stipulated otherwise. Under some circumstances, a written consent is required.

It is worth to know that when it is necessary for personal information processors to provide personal information outside of the territory of the People's Republic of China, the processors must meet one of the following conditions: passing safety assessment organized by the competent government authority; obtaining Personal Information Protection Certification issued by authorized professional institutions; adopting the template contract formulated by competent government authority ; or other conditions stipulated by law or regulation.

Criminal Law

To prevent and fight against crime of infringe data safety, Criminal Law stipulates several crimes.

- Crime of infringing upon citizens' personal information. Any organization or individual violates the relevant laws and regulations to sell personal information of citizens to a third party shall be imposed a fine, and/or sentenced to criminal detention or fixed-term imprisonment, which can be as long as no more than 7 years.

- Crime of refusing to perform the obligation to manage information network security. The object of this crime is internet service providers, which provide information to the public or provide services to the people who intend to obtain internet information. The providers may be imposed a fine, and/or sentenced to criminal detention or no more than 3 years fixed-term imprisonment if they refused to correct their security measures under the requirement of the competent supervision authority so as to cause: widespread of illegal information; serious harm by disclosure of users' information; serious harm due to the loss of evidence in a criminal case; or other serious circumstances.

Administrative Law System

From the perspective of strengthening the administration of data by the government, China has also

introduced a series of laws, the most important of which are Cybersecurity Law (effective on 1st June, 2017) and Data Security Law (effective on 1st September, 2021).

Purpose

We can see the common purposes of the two laws: both aim to the safeguard of national security (Data Security Law adds sovereignty security), and the protection of the legal rights of individuals and organizations. On the other hand, the two laws aim to the protection of network and data, as well as to promote the development and utilization of data and information technology.
This is a good example shows the effort by the PRC government to balance the benefit and negative impact arising from the development of new technology.

Cybersecurity Law

All the organizations or individuals that construct, operate, maintain, and use the network within the People's Republic of China, as well as the supervision and management of network security are subject to this law. The PRC government implements network security level protection rules. Network operators should fulfil their security protection obligations in accordance with the rules to protect the network from interference, sabotage, or unauthorized access, and to protect network data from being leaked, stolen, or tampered.

The PRC government implements the key protection for those important industries and fields, such as public communications, information services, energy, transportation, water conservancy, finance, public service, and e-government, as well as the key information infrastructure, which could seriously endanger national security, national economy, and the people's livelihood and public interests if it is destructed, loss of functionality or data leakage.

It is required that the operators of key information infrastructure must store any and all personal data collected and generated during its operating in the People's Republic of China. The State Council is authorized by the law to formulate the specific scope and security protection measures for critical information and infrastructure. By now, we have not seen any specific measures by the State Council.

There is a similar stipulation (Art. 40) in the *Personal Information Protection Law*, which mentioned that the key information infrastructure operators and personal information processors shall store the data domestically collected and generated within the People's Republic of China when the processed amount of personal information reaches a certain amount. We have not found out how much "the certain amount" is yet but it is believed that the government will classify according to the importance and sensitivity of the data, not just amount of data. For example, Apple and Tesla are both required to store the data in China, although the number of customers of these two companies are far apart.

Data Security Law

The law advocates Big Data Strategy. The government will promote the construction of data infrastructure, encourage and support the innovative application of data in various industries and fields. The state will support the development and utilization of data to improve the intelligent level of public services. This strategy will lead to innovative and profitable business in this field.

This law stipulates that the state protects data based on different types and levels of data classified according to the importance in social and economic

development, and to the extent of harm that may be caused to national security, public interests or legal rights of organizations and individuals.
The law also stipulates the obligations of data processors. It is required that any process of data or development of new data technology must be aimed to promote economic and social development, improve people's common wealth and accord with social morality and ethics.

+ + +

ALLIURIS

The ALLIURIS GROUP consists of 20 law firms and 400 business lawyers within Europe, Asia and America. (www.alliuris.law).

……..

Your contact:
Alisha Daley-Stehr,
Alliuris Communication

info@alliuris.org
Fon 0049-511-307 56-0
Fax 0049-511-307 56-10

……..

China

Guangdong J&J Law Firm
14th Floor, Industrial Bank Building,
101 Tianhe Road, Tianhe District,
Guangzhou
China

Fon +86 20 – 85608818
Fax +86 20 – 38988393

Mail jennifer@gdjunhou.com
Mail zjw@gdjunhou.com
Web www.gdjunhou.com

Languages: Chinese, English
Contact Person: Jennifer Feng, Senior Partner
Contact Person: Joe Chow, Managing Partner

……..

IMPRINT

EDITORS

ALLIURIS A.S.B.L.
ALLIANCE OF INTERNATIONAL BUSINESS LAWYERS
BRUSSELS

MANAGEMENT
Luisenstr. 5, D-30159 Hannover
Fon +49-511-307 56-50 505056-20 Fax +49-511-307 56-60

BRUSSELS · KNOKKE · PARIS · LONDON · AMERSFOORT · UTRECHT · LUXEMBURG · LYON · MADRID · BARCELONA · LISBON · MILAN · COPENHAGEN · HANOVER · ZUG · VIENNA · SALZBURG · KRAKOW · MOSCOW · MINSK · ATHENS · ISTANBUL · BEIJING · SHANGHAI · GUANGZHOU · NEW DELHI · MUMBAY · NEW YORK · MEXICO CITY SAO PAULO · RIO DE JANEIRO · BRASILIA · BUENOS AIRES · LIMA

EDITORIAL DEPARTMENT
Ulrich Herfurth, Rechtsanwalt