

Прокурорский надзор. Судебная система

Участие прокуратуры Китая в судебном процессе в общественных интересах по защите личной информации (часть 1) Chinese Procuratorial Public Interest Litigation on Personal Information Protection (Part 1)

Чжан Цзихун,
профессор Шанхайского университета
политических наук и права,
г. Шанхай, Китай
pangdongmei71@163.com

Цао Ицзюнь,
аспирант кафедры международного права
Шанхайского университета
политических наук и права,
г. Шанхай, Китай
pangdongmei71@163.com

Zhang Jihong,
Professor of Shanghai University
of Political Science and Law,
Shanghai, China
pangdongmei71@163.com

Cao Yijun,
Postgraduate of International Law,
Shanghai University
of Political Science and Law,
Shanghai, China
pangdongmei71@163.com

© Чжан Цзихун, Цао Ицзюнь, 2022

DOI: 10.17803/2587-9723.2022.5.025-036

Аннотация. Закон о персональных данных Китайской Народной Республики был официально введен в действие 1 ноября 2021 г. Закон воплощает идею развития, ориентированного на людей, и представляет китайский опыт решения проблем защиты личной информации, с которыми сталкивается международное общество. Статья посвящена развитию китайского Закона о персональных данных, объясняет цель принятия данного Закона, его основных положений и характеристики. Кроме того, в статье делается акцент на ведении судебных разбирательств по защите личной информации, указываются недостатки этой системы с целью ее совершенствования и развития.

Ключевые слова: защита персональной информации, судебный процесс, прокуратура, обработка персональной информации.

Abstract. The Personal Information Protection Law of the People's Republic of China (hereinafter referred to as Personal Information Law) has been officially implemented on November 1, 2021. The birth of this law embodies the idea of people-centered development and provides Chinese experience and solutions for the personal information protection problems faced by international society. This article focuses on the development of Chinese personal information law and explains the legislative purpose of Personal Information Law to further show seven highlights and two characteristics of it.

Also, it puts emphasis on introducing Chinese procuratorial public interest litigation on personal information protection and points out the shortcomings of this existing system with a view to perfecting and developing the system value maximally.

Keywords: Personal Information Protection; Procuratorial Public Interest Litigation; Personal Information Processing.

Introduction

Emerging Internet, communication and AI technologies have aroused public attention during the unprecedented development in the era of big data. While people are enjoying the speed and convenience brought by technology, the security issue of frequent leakage of personal information has become increasingly critical. To effectively deal with such information leakage threats, most countries have introduced their own relevant legislation on data, personal information, and privacy protection. After years of preparation, Chinese own Personal Information Protection Law finally came into effect on November 1, 2021. The basic starting point of the law is to protect the rights and interests of personal information, regulate personal information processing, and to promote the rational use of personal information. There are outstanding highlights in the law, including standardizing the basic rules of personal information processing and automated decision-making, strictly protecting sensitive personal information, offering information subjects full rights, strengthening the basic obligations of personal information processors, providing stricter legal liabilities and firstly establishing Chinese procuratorial public interest litigation on personal information protection. This law also demonstrates two distinguishing characteristics — modernity and locality, condenses Chinese wisdom while absorbing the global advanced experience, and gets closer to Chinese reality.

It is worth mentioning that Personal Information Law has built procuratorial public interest litigation on personal information protection in China for the first time, where procuratorates shoulder the important responsibility of protecting national interests and social public interests. As citizens' demands grow for the protection of personal information, procuratorate ought to actively respond to these to give full play to the function of procuratorial public interest litigation, enabling this system to develop its due value maximally on personal information protection.

1. Legislative evolution of Chinese Personal Information Law

1.1. The development of Chinese Personal Information Law

Personal information used to be firstly regulated by Criminal Law in China, which focuses on the collection, use and protection of personal information. As early as in 2005, Amendment (V) to the Criminal Law of the People's Republic of China added the crime of stealing, buying, and illegally providing credit card information, aiming to crack down on criminals obtaining or exchanging money, material, etc. for other people's credit card information by secret means or privately providing other people's credit card information. This is the first regulation concerning violations of citizens' personal information in China.¹

In 2009, Amendment (VII) to the Criminal Law of the People's Republic of China included stealing or otherwise illegally obtaining, selling or illegally providing citizens' personal information into the scope of criminal crackdowns for the first time, but the crime subject was limited to the staff of state agencies or financial, telecommunications, transportation, education, medical and other units. Subsequently, Amendment (IX) to the Criminal Law of the People's Republic of China made further improvements to the above provisions in 2015, cancelling the original restrictions on the criminal subject and extending the scope to all natural persons, and severely punished those who obtain citizens' personal information in the process of performing duties or providing services selling or providing it to others.

In 2013, China amended Law of the People's Republic of China on the Protection of Consumer Rights and Interests, which gave consumers the right to protect their personal information and added the civil liability of operators for infringement of consumers' personal information rights in the follow-up provisions. This is the first time that Chinese law regulated personal information from the perspective of civil rights.² In fact, the situation of personal information leakage is particularly worsening in China. Due to the status quo of heavy losses to victims, especially the case that Xu was cheated of tuition fees because of information leakage, causing sudden illness and

¹ See Yu Hai-Song. Twenty Lectures on Cybercrime Law [M]. Beijing, Law Press, 2018 .P. 203.

² See Cheng Xiao. Understanding and Application of the Personal Information Protection Law [M]. Beijing, Chinese legal system press, 2021. P. 5.

death that in 2016 has had a disastrous impact on society, the provisions have been further promulgated on the protection of personal information in Article 111 of General Principles of the Civil Law of China.³

Although there remain disputes over the personal information rights of natural persons in Chinese theoretical circles, Article 111 of General Principles of the Civil Law still clarifies that it should be protected in the light of the civil basic law.⁴ Therefore, in the subsequent formulation of Civil Code, China completely retained Article 111 of General Principles of the Civil Law and Privacy Right and Personal Information Protection in a special chapter in the edition of personal information rights, introducing more detailed regulations on the protection of personal information.

In addition, China pays meticulous attention to the protection of personal information in specific fields. For example, Cyber Security Law implemented in 2017 focuses on regulating the collection, storage and use of personal information in the field of cyberspace. E-commerce Law, promulgated in 2018, also clarified that in the process of precision marketing to consumers through big data, e-commerce operators should provide consumers with options that are not specific to their personal characteristics, so as to protect consumers' right to know and right to choose.

Although numerous laws in China provide corresponding regulations on the protection of personal information in terms of criminal liability and civil protection, China still needs to formulate a unique Personal Information Protection Law to comprehensively protect natural persons' personal information. With the continuous in-depth integration of informatization and economic society, the network has become a new space for production and life, a new engine for economic development, and a new link for exchanges and cooperation. As of March 2020, China has 900 million Internet users, more than 4 million Internet websites, and more than 3 million applications.⁵

The collection and use of personal information is more extensive. Although the protection of personal information in our country has been increasing in recent years, in real life, some enterprises, institutions and even individuals, based on commercial interests, randomly collect, illegally acquire, excessively use, illegally buy and sell personal information, and use personal information to invade the people. Issues such as the peace of life of the masses and endangering the lives and health of the masses and the

safety of their property are still very prominent. In the information age, the protection of personal information has become one of the most immediate and practical interests of the people. From a worldwide perspective, specific personal information protection legislation is the mainstream.

Since the beginning of 21st century, great achievements have been made in the construction of Digital China. Both the information infrastructure construction and the innovation capability of information technology occupy the pre-eminent position in the world. The development and construction of Digital China cannot be divorced from adequate legal safeguards, since the formulation of the Personal Information Protection Law does not only conform to international standards and international situation, but also can build a personal information protection legal system compatible to Chinese characteristics. Accordingly, on August 20, 2021, the Personal Information Protection Law was reviewed and passed, and it came into effect on November 1 of the same year.

The promulgation of the Personal Information Protection Law will considerably strengthen the legal protection of Chinese personal information protection, forming a more complete system in the protection of personal information and providing stronger legal protection. Furthermore, the main purpose of this law lies in scientifically coordinating the relationship between the protection of personal information rights and the rational use of personal information, which establishes personal information processing rules with clear rights and responsibilities, effective protection, and standardized use. It also promotes the free and safe flow and effective use of personal information as well as protects the rights and interests, thus facilitating the healthy development of Chinese digital economy.⁶

1.2. The legislative purpose of Chinese Personal Information Law

A clear conception of the legislative purpose is conducive to a deeper understanding of the rules and systems in the law, helping apply the corresponding legal norms more accurately. Meanwhile, it enables pertinent administrative agencies and local governments to formulate corresponding laws and regulations, on the premises that they accurately grasp the purpose of legislation. On that account, the provisions of the law can be implemented thoroughly, and the court can interpret the law more accurately based on

³ See *Yang-Lixin*. Personal Information: Legal Interests or Civil Rights- Interpretation of Personal Information Stipulated in Article 111 of the General Principles of Civil Law [J] *Legal Forum*. 2018 (1). P. 36.

⁴ See *Zhang-xinbao*. Research on Personal Information Protection Provisions of General Principles of Civil Law [J] *Chinese and Foreign Law*. 2019 (1). P. 63.

⁵ See China National People's Congress. Explanation on the Personal Information Protection Law of the People's Republic of China (Draft) // URL: <http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml>.last visited on December 2, 2021.

⁶ See *Cheng Xiao*. Op. cit. P. 7.

the legislative purpose in judicial judgments.⁷ Overall, Chinese Personal Information Protection Law is established for the following three legislative purposes.

1.2.1. Protecting the rights and interests of personal information

According to Personal Information Law, personal information refers to various types of information related to an identified or identifiable natural person. It is recorded by electronic or other means, and does not include anonymized information. As to the definition of personal information, Chinese defines it in a way similar to the alternative employed by GDPR. All personal information associated with identifiable natural persons is taken into the scope of adjustment, and relatively enlarges the scope of protection. The reason why China and GDPR share the approach to definition is that it can still exert a dramatic impact on it in the Internet and big data era,⁸ even if the amount of information cannot directly help identify the name, address and phone number of the information subject. In other words, if the information is not linked to an identified or identifiable natural person, it will not belong to the category of personal information, and it cannot be applied with the Personal Information Protection Law or other Chinese laws on the protection of personal information. It is because only the collection, use, disclosure and other processing activities of personal information may damage the basic rights of natural persons, like the dignity of the person. Above all, it is very reasonable to distinguish between identifiable or identifiable personal information and unidentifiable information. In the modern information society, if the law adopts the same protection mode for the processing of all information, it will result in the excessive protection, such as blocking the flow of information and affecting the prosperity of the digital economy, which will ultimately harm national and social public interests.

Therefore, the primary legislative purpose of the Personal Information Protection Law is to protect people's individual information rights from infringement. The Personal Information Protection Law makes many systematic provisions in the formulation of the provisions around this legislative goal. For example, it establishes the basic principles that must be followed in personal information processing activities, including lawfulness, fairness, necessity, integrity, etc., stipulates the rights that the information subject should enjoy in the process of personal information processing activities, and constructs a complete obligation system for personal information processors, with the intention of fully protecting the

personal information rights and interests of natural persons.

1.2.2. Regulating personal information processing activities

Personal information processing activities mean the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information. The Personal Information Protection Law copes with the handling of personal information with a full range of regulations; otherwise, no matter which method information processors utilize or which purpose they intend to fulfill, as long as they process personal information, all should be regulated by the Personal Information Protection Law. However, some Chinese scholars argue that the Personal Information Protection Law should be limited to the collection, control, sharing, analysis and application of personal information for the purpose of identification and analysis instead of designated to regulate all personal information processing behaviors. Only these actions will exert a relatively significant impact on the rights and interests of information subjects, as for the general use of personal information should be left to other laws or industry standards or social norms to adjust.⁹

There is a certain irrationality in this view. Firstly, there are many types of personal information processing methods, including collection, storage, use, processing, uploading, etc. Each of these parts contains the risk of infringing upon the rights and interests of natural people, and they cannot be separated unilaterally.¹⁰ Secondly, as the result of scientific and technological development, more new types of personal information processing methods will emerge in the future, while attendant risks become even more unpredictable. The risks in personal information processing are per se multiple, which is not limited to processing actions for the purpose of identification and analysis. Moreover, personal information processing is changeable and developmental, so the display of the current processing behavior without the purpose of identification analysis does not indicate that such behavior will not be carried out in the future, nor does it mean that it will not pose a risk to the rights and interests of personal information.

1.2.3. Promoting the rational use of personal information

Throughout the world, all countries and regions have formulated personal information protection laws and regulations and further covered this legislative purpose. For instance, the Personal Data Protection Law in Taiwan clearly declares the legislative

⁷ See *Cheng Xiao*. Op. cit.

⁸ See *Ronald Leenes*. Do they know me? Deconstructing Identifiability [J] *University of Ottawa Law & Technology Journal*. 2007 (4). P. 135.

⁹ See *Gao-Fuping*. Personal Information Processing: Standard Objects of Chinese Personal Information Protection Law [J] *Legal Business Research*. 2021 (2). P. 78.

¹⁰ See *Cheng Xiao*. Op. cit. P. 13.

purpose of this law — to “regulate the collection, processing and use of personal data...and promote the rational use of personal data”. GDPR, Japan, Brazil and other countries all share their provisions in their personal information protection legislation. It can be found that the common practice in the world is to pay attention to the coordination between the protection of civil rights and interests of personal information and the protection of reasonable freedom. It touches upon the respect and protection of basic human rights, namely the dignity of natural persons. Additionally, it is concerned with effective safeguard for public interests and business activities and the freedom of speech and information circulation.¹¹

It should be said that personal information is not only attached to the personal dignity and freedom of the individual, but also carries the legitimate interests and public interests of the personal information processor. Specifically, the personal information protection system not only protects the rights and interests of personal information, but also promotes the rational use and circulation of personal information. Enterprises, governments and other organizations have the right to collect and process personal information based on legal provisions or agreements. When the realization and maintenance of public interest requires the use of personal information, such as the collection of the track information of confirmed or suspected patients during the epidemic, the acquisition of personal information required for criminal investigation, prosecution, or trial, etc., it can also be used directly without consent. This not only protects the legitimate rights and interests of other subjects in the society and the needs of public interests, but also helps directly or indirectly promote social welfare.¹²

By the same token, Chinese Personal Information Protection Law is not only meant to protect the rights and interests of personal information, but also highly linked to the rational use of personal information. In the meantime, Chinese law circles have widely reached a consensus that the balance should be stricken between the protection of natural persons' rights and interests and the rational use of personal information or personal data. In other words, when the rights and interests of personal information are protected, attention should also be paid to the promotion of the rational and effective use of information and data in accordance with the law. In that case, the law circles can facilitate the sustainable and healthy development of Chinese digital economy.

For example, not only does Chinese Personal Information Protection Law stipulate the basic principle that the information processor should notify and obtain the information subjects' consent when

processing personal information, but it also enumerates the exceptions for legal processing of personal information without consent in the same clause, including but not limited to fulfilling contractual obligations, performing statutory duties or statutory obligations, responding to public health emergencies, etc. Plus, what needs to be emphasized further is that the handling of personal information under exceptional circumstances still needs to strictly abide by the processing rules stipulated by the law, and to fulfill personal information protection obligations.

To this end, the Personal Information Protection Law not only clarifies that this law is applicable to the activities of handling personal information in China, but also draws on the practices of relevant countries and regions to endow the Personal Information Protection Law with the necessary extraterritorial validity to fully protect the rights and interests of individuals in China. The Personal Information Protection Law stipulates that it is also applicable to personal information processing activities that occur outside of China for the purpose of providing products or services to domestic natural persons, or for analyzing and evaluating the behavior of domestic natural persons. And overseas personal information processors set up specialized agencies or designated representatives in China to be responsible for matters related to personal information protection.

In summary, it can be found that the Personal Information Protection Law is a product of insisting on combining Chinese national conditions and drawing on international experience. Proceeding from Chinese actual conditions, it will thoroughly summarize the implementation experience of laws, regulations, and standards such as the Cybersecurity Law, and elevate effective practices and measures to legal norms. Since the 1970s, the Organization for Economic Cooperation and Development, the Asia-Pacific Economic Cooperation Organization, and the European Union have successively issued personal information protection related guidelines, principles and regulations, and more than 140 countries and regions have formulated the personal information protection laws.¹³

The Personal Information Protection Law fully draws on the useful practices of relevant international organizations, countries and regions, and establishes a sound legal system that meets the needs of Chinese personal information protection and the development of the digital economy. At the same time, the Personal Information Protection Law insists on combining problem-oriented and legislative foresight. Based on the outstanding problems existing in the field of personal information protection and the major concerns

¹¹ See *Cheng Xiao*. Op. cit. P. 14.

¹² See *Zhang-Jihong*. The Draft of Personal Information Protection Law that Reflects the Voice of the People, Shanghai People's Congress Monthly. 2021 (5). P. 52.

of the people, establish a sound and feasible system and norms.

For some still controversial theoretical issues, the Personal Information Protection Law will leave necessary space, and for new issues brought about by new technologies and applications, necessary provisions will be made on the basis of full research and demonstration to reflect the inclusiveness and forward-looking nature of the law. Finally, the Personal Information Protection Law also pays attention to handling the relationship with relevant laws. Grasp the legislative positioning of the protection of rights and interests, link up with the relevant laws and regulations such as the Civil Code, and refine and enrich the personal information protection system rules. At the same time, in conjunction with the Cyber Security Law and the Data Security Law, the Personal Information Protection Law no longer makes provisions for the network and data security supervision-related system measures established by the Cyber Security Law and the Data Security Law.

2. Highlights and features of Chinese Personal Information Protection Law

2.1. Seven highlights of Chinese Personal Information Protection Law

2.1.1. *Standardizing the basic rules of personal information processing*

Chinese Personal Information Protection Law clearly stipulates that the processing of personal information must have legal grounds. In the past, the basic premise of information processors' processing personal information is the information subjects' consent, while the current Personal Information Protection Law takes into account the complexity and diversity of the personal information processing environment, and starts from the perspective of maintaining public interests and good social order. In that case, provisions are made for special circumstances under which personal information can be legally processed without obtaining personal consent to ensure the scientific accuracy and preciseness of legislation, including but not limited to the discharge of contractual obligations, the fulfillment of statutory duties or statutory obligations, the response to emergencies, and the supervision of news reports or public opinion.

The Personal Information Protection Law has also established personal information processing rules centered on "inform-consent", requesting the information

subjects' voluntary and explicit consent to be obtained on the premise of full notification before processing personal information. When important conditions are changed such as the purpose, method, and type of information for processing personal information, the information subjects' consent should be re-obtained. At the same time, individuals are given the right to withdraw such consent at any time. Personal information processors must not only provide individuals with a convenient way to withdraw their consent, but once the individual withdraws their consent, the personal information processor should stop processing or delete personal information in a timely manner. It should also be noted that China has put forward stricter and more detailed requirements in the consent regulation than GDPR has done, distinguishing between different applicable situations such as consent, individual consent and written consent. To take one example, processing sensitive personal information requires the individual consent of the information subject. In comparison, GDPR does not take similar prerequisites, but it requires that the consent given by the information subject should be fully informed or undisputed.¹⁴

More stringent statutory conditions are stipulated for the processing of minors' personal information under the age of fourteen, the processing of personal sensitive information, the joint processing of personal information, the entrusted processing of personal information, and the transfer of personal information across borders.

Regarding the subject of personal information processing, special regulations are imposed on the processing behavior of state agencies. The processing of personal information by state agencies has the characteristics of public welfare and authority, and is significantly different from the commercial and autonomous nature of processing personal information by other legal persons and unincorporated organizations. In view of this, the Personal Information Protection Law set up a special section to stipulate the rules for the handling of personal information by state agencies, emphasizing that the state agencies perform statutory duties to process personal information. Normally, they follow the "inform-consent" rules, but excluding that laws and administrative regulations require confidentiality or informed consent will prevent the performance of statutory duties. At the same time, the personal information processed by state agencies should be stored in China, and risk assessment should be conducted if it is really necessary to provide it overseas. It is worth noting that the Personal Information Protection

¹³ See China National People's Congress. Explanation on the Personal Information Protection Law of the People's Republic of China (Draft) // URL: <http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml>. last visited on December 2, 2021.

¹⁴ See Tencent Research Institute. Comparison of Personal Information Protection Laws in China, the United States and Europe-Taking China's Personal Information Protection Law, EU GDPR, and California CCPA&CPRA as samples // URL: <https://www.tisi.org/19493>. last visited on December 2, 2021.

Law emphasizes that state agencies should perform statutory duties to process personal information in accordance with statutory powers and procedures, and must not exceed the scope and limits necessary to perform statutory duties. This content effectively responds to the public's worries and anxiety about the abuse of power by public authorities to obtain personal information.¹⁵

2.1.2. Prohibiting big data-enabled price discrimination against existing customers and standardizing automated decision-making

Today, more and more companies are skilled in evaluating the personal characteristics of consumers with the help of big data, and transform that into their own marketing tool. They will use information such as consumers' consumption habits, consumption levels, and sensitivity to prices to impose differentiated and discriminatory treatments on consumers in terms of transaction prices, which even misleads consumers in terms of prices and maximizes the benefits of companies' own business. This is exactly the big data-enabled price discrimination against existing customers that has been prominently reflected in the society in recent years.

Such tactic does not only violate the principle of good faith in the sense of civil law, but also seriously infringes consumers' right to fair transactions. The Personal Information Protection Law requires that personal information processors should ensure the transparency of decision-making and the fairness and impartiality of the results. They must not impose unreasonable differential treatment on individuals in terms of transaction prices and other transaction conditions in the process of reach automated decisions through utilizing personal information. In fact, before the Personal Information Protection Law enacted legislation to prohibit this phenomenon, Chinese Anti-Monopoly Law also had clear provisions on this, taking the phenomenon as an abuse of market dominance. The way Personal Information Protection Law stipulates the phenomenon of big data-enabled price discrimination against existing customers does not only actively respond to the hot issues of social and people's livelihood, but also provides a new protection path for the increasingly frequent phenomenon outside anti-monopoly regulations. After all, the activities of personal information processing play the most fundamental supporting role in the issue. Without personal information processing, the big data-enabled price discrimination against existing customers can barely occur. In conclusion, the Personal Information Protection Law plays a key role in solving above problems through the regulation of activities in personal information processing.

2.1.3. Strictly protecting sensitive personal information

The Personal Information Protection Law divides personal information into general personal information and sensitive personal information, and has formulated different rules about information processing based on their characteristics. Sensitive personal information is referred to as biometrics, religious beliefs, specific identities, medical health, financial accounts, whereabouts as well as personal information of minors under 14 years of age. The main reason why Personal Information Protection Law classifies data like above is that once the above-mentioned information is illegally used or leaked, the natural person's individual dignity, property safety and personal safety will be clearly exposed to irreversible and serious violations. Therefore, information processors must cautiously handle this type of sensitive personal information.

There is also a special chapter in Personal Information Protection Law on the processing rules of sensitive personal information. Information processors are required to process natural persons' sensitive personal information only if they display a specific purpose and sufficient necessity, and the individual's consent should be obtained separately in advance, informed of the necessity of processing sensitive personal information and the possible impact on their personal rights and interests, and adequate protection measures also should be taken. Furthermore, it is worth noticing that the Personal Information Protection Law also covers the personal information of minors under the age of 14 in the category of sensitive personal information, demanding the information processor to obtain the consent of the minor's parents or other guardians when processing the above information and formulating special personal information processing rules. This is not only to fully protect the personal information rights and physical and mental health of minors, but also to converge with the relevant provisions in Minors Protection Law.

2.1.4. Giving individuals full rights

It is generally believed in comparative law that the purpose of protecting personal information is to protect the self-determination of individuals on their personal information. In civil law countries, this right originated in Germany. In 1976, the German scholar Christoph Mallmann took the lead in proposing the "right to personal information self-determination" (das Recht auf informationelle Selbstbestimmung), who believed that personal information is of great significance to the development of personal personality and is a medium for personal self-expression (Selbstdarstellung) and communication with the social environment.¹⁶

¹⁵ See Zhang-Jihong. Op. cit. P. 52.

¹⁶ Quoted from Wang-Liming & Ding-Xiaodong. On the Highlights, Features and Application of Personal Information Protection Law [J] The Jurist. 2021 [6]. P. 4.

Therefore, based on the right to self-determination, right holders should have the right to give informed consent to personal information. The right of personal information self-determination is also generally accepted by the two major legal systems. This right is also the theoretical basis for personal information protection. Other rights related to personal information protection are derived from this right.

Nowadays, China takes initiative to explore diversified ways of personal information governance, while the rights that individuals own over their personal information are also amongst the essential types of personal information protection. For this reason, Personal Information Protection Law refers to the relevant provisions of foreign personal information protection laws represented by GDPR, and fully stipulates the rights of individuals in personal information processing activities. Specifically, the Personal Information Protection Law clarifies that individuals have the right to know and take decisions about the processing of their personal information, and the right to restrict or refuse the processing of their personal information by others; the right of inspection, reproduction, and portability; the right to correct; the right to delete; the right to request interpretation, to help information subjects better manage their information rights and interests, as well as risk anticipation and prevention.¹⁷

As for the death of a natural person, it is also clear that close relatives can exercise personal information rights of the deceased. With the simultaneous advancement of digitization and aging, the protection of the personal information of the deceased has become the focus of attention of all parties. Although whether the deceased has personality interests based on personal information, it is still a controversial issue in academic circles. The legislation and judicial practice of various countries are cautious about the protection of the deceased's personal information. Chinese Personal Information Protection Law has taken another step forward on the basis of the tort relief mechanism established by the Civil Code.

It clearly recognizes the deceased's personal information interests in the legislation and proposes a specific protection mechanism—that is, by the deceased's close relatives. For their own lawful and legitimate interests, the deceased's personal information may be lawfully exercised with the rights of access, reproduction, correction, deletion, etc., as required by law, unless otherwise arranged by the deceased during his lifetime. Of course, considering that in real life, there is a large amount of personal information that has intersecting attributes, and it also involves

the privacy and personal information interests of the other people, such as communication content, email information, etc. If it is generally used by close relatives, it may cause harm to the opposite party. Privacy infringement and data security risks require a more detailed stipulations of future practices.¹⁸

On the whole, Chinese Personal Information Protection Law provides relatively comprehensive provisions on the rights of individuals in personal information processing activities. Except for the current disputed right to be forgotten, which is not clearly stipulated in the academic circles, the rest are generally involved. It is consistent with international legislation.

Furthermore, the Personal Information Protection Law introduced the right to portability of personal information for the first time. Where individuals request the transfer of personal information to the designated personal information processor to meet the conditions specified by national cyberspace administration, the personal information processor shall provide the means for the transfer. In fact, the right to portability of personal information was pioneered by GDPR and reflected in the legislation of the United States, Australia and other countries.

However, the establishment of the right to portability in Chinese legislation is a conditional and restricted right. To a certain extent, there is a certain degree of commonality with the provisions of the GDPR. Considering that the Personal Information Protection Law, like the EU GDPR, is a comprehensive and general law applicable to various institutions in the public and private sectors, including state agencies, hospitals, banks, etc. The issue of data transferability between these subjects is inherently more complicated. In fact, the right to portability has always been a more controversial topic, involving the privacy protection, data security and market competition of third-party users. So far, there is no clear conclusion. Even the EU GDPR, which was the first to introduce data portability, has not yet implemented a specific plan.

In practice, there is a large amount of personal information related to the privacy protection of others, such as mobile phone address books, call records, and chat information transfer records. If one user is given the right to directly transfer such information, other individuals involved in the information have no chance to know their own data has been submitted to the new data processor by others, and thus has no chance to exercise their rights. Even between different businesses within an enterprise, supporting users to directly transfer such information may also

¹⁷ See Ari Ezra Waldman. Privacy as Trust: Sharing Personal Information in a Networked World [D] University of Miami Law Review. 2015. P. 560—590.

¹⁸ See Tencent Research Institute. Comparison of Personal Information Protection Laws in China, the United States and Europe-Taking China's Personal Information Protection Law, EU GDPR, and California CCPA&CPRA as samples. <https://www.tisi.org/19493>. last visited on December 2, 2021.

cause serious privacy protection issues. For example: Google once arbitrarily defaulted users to transfer google gmail address book information directly to its social service google buzz, which was severely fined by the FTC. In the process of transferring from a mutually independent platform to another, how to allocate responsibilities between the transmitter and the receiver? Who is ultimately responsible for the security of the transferred data? Before these problems are resolved, the hastily introduction of portability rights may bring greater security risks. One of the problems exposed by the Facebook scandal is that the platform is too open to the user's policy of disclosing and migrating personal data to third parties, which ultimately leads to security incidents.¹⁹

2.1.5. Strengthening the basic obligations of personal information processors

The emergence of large-scale network platforms and super-large network platforms exponentially increase the dependence of information subjects on them.²⁰ As the primary person responsible for the protection of personal information, personal information processors should abide by the obligations set by the Personal Information Protection Law when handling personal information activities. Personal information processors shall adopt strict security protection measures when conducting personal information processing activities, formulating realistic internal operating procedures and specifications, regularly conducting compliance audits on personal information processing activities.

They also need to conduct prior impact assessments on high-risk processing activities such as processing sensitive personal information, automated decision-making, providing or disclosing personal information. For those personal information processors that process personal information up to the number prescribed by the national cybersecurity administration, a person in charge of personal information protection should also be designated to supervise personal information processing activities and protective measures taken.

As some large-scale Internet platforms provide a large number of technical support and processing rule settings for information processors to process

personal information, Internet platforms play a pivotal role in the processing of personal information and are an important link in the protection of personal information. So, Article 58 of the Personal Information Protection Law stipulates special obligations for these large Internet platforms, including establishing a personal information protection compliance system, formulating platform rules, regularly publishing personal information protection social responsibility reports, etc.

More than that, the Personal Information Protection Law also provides for the personal information protector system. According to Article 52 of the Personal Information Protection Law, personal information processors that process personal information up to the number prescribed by the national cyberspace administration shall appoint a person in charge of personal information protection to be responsible for supervision on personal information processing activities as well as protective measures taken, among others. The personal information protection officer system is similar to the Data Protection Officer (DPO) system of the European Union and other countries and regions.

The core of the establishment of this system is to promote the professionalism and independence of corporate personal information protection and strengthen the company internal data governance. At present, many companies in China have set up dedicated data protection positions or personnel internally. Some government departments have also conducted trials. For example, Guangdong Province has issued the Guangdong Province Chief Data Officer System Pilot Work Plan to pilot the establishment of a chief data officer system, innovate data sharing and openness and development and utilization models, and improve data governance and data operation capabilities.²¹

Shenzhen has also issued the Shenzhen Chief Data Officer System Pilot Implementation Plan, which will pilot the establishment of chief data officers in 8 municipal units including the city's own government, Futian and other 4 district governments, and the municipal public security bureau to improve data governance and data operation capabilities help

¹⁹ See Tencent Research Institute. Comparison of Personal Information Protection Laws in China, the United States and Europe-Taking China's Personal Information Protection Law, EU GDPR, and California CCPA&CPRA as samples // URL: <https://www.tisi.org/19493>. last visited on December 2, 2021.

²⁰ See *Friso Bostoen*. Neutrality, Fairness or Freedom? Principles for Platform Regulation [J] *Internet Policy Review*. 2018. P. 1—19.

²¹ In May 2021, the Guangdong Province Chief Data Officer System Pilot Work Plan was officially issued. Guangdong Province selects six provincial departments including the Provincial Public Security Department, the Provincial Department of Human Resources and Social Security, the Provincial Department of Natural Resources, the Provincial Department of Ecological Environment, the Provincial Medical Insurance Bureau, and the Local Financial Supervision Bureau, as well as Guangzhou, Shenzhen, Zhuhai, Foshan, Shaoguan, Heyuan, Zhongshan, Jiangmen, Maoming, Zhaoqing and other 10 prefectures and cities carried out pilot work to promote the establishment of a chief data officer system and deepen the reform of market-oriented allocation of data elements.

Shenzhen's smart city and digital government construction.²² At the same time, in accordance with the provisions of Article 53 of the Personal Information Protection Law, in the activities of processing the personal information of natural persons in the People's Republic of China outside the People's Republic of China, special agencies or designated representatives shall also be established in China in accordance with the law to be responsible for handling personal information protection related activities or matters.

2.1.6. Providing stricter legal responsibilities

In the face of new problems and new situations in the protection of personal information under the background of new technologies, the Personal Information Protection Law comprehensively uses public relief, private relief, social relief and other methods to realize the comprehensive protection of personal information. The subjects of personal information processing activities are diverse, involving a wide range, and are highly concealed so that it becomes quite difficult for administration to supervise, and the consumption of administrative resources also keeps heavy.

Besides, once a large-scale incident of infringement of personal information occurs, it will cause severe damage to the originally good and stable social order. Based on foreign experience and the characteristics of personal information protection itself, severe penalties for violations of personal information conform to legal logic. At the level of administrative responsibility, the Personal Information Protection Law provides a comprehensive administrative punishment mechanism, including warnings, ordering corrections, confiscating illegal gains, fining, revoking business licenses, etc. Among them, the fines imposed on a company can be as high as 5% of the company's turnover in the previous year, and there also stipulate corresponding prohibitions on employment for directors, supervisors, senior managers and personal information protection persons of the companies involved.

Concerning civil liability, the Personal Information Protection Law provides the principle of presumed fault liability and inverted evidential burden. Where rights and interests on personal information are infringed due to any personal information processing activity and the personal information processors cannot prove that they are not at fault, the personal information processors shall assume liability for damages and other tort liability.

2.1.7. Firstly establishing Chinese procuratorial public interest litigation on personal information protection

In the era of networks, the scale of personal information processed by information processors is so large that it has covered a wide range of natural persons. Once there is an illegal processing, the legitimate rights and interests of many natural persons will be infringed. In practice, because the infringement behavior of information processors is often hidden, and such infringement will not directly cause damage to the rights and interests of a specific natural person, it will affect the public interests of unspecified subjects.

Therefore, a single individual rarely initiates a lawsuit without a direct interest. Even if the victim intends to initiate a lawsuit, the high litigation cost often dampens the victim's enthusiasm for rights protection. In that case, it is very necessary to establish a public interest litigation system on personal information protection, which is a positive response to hot social issues and focuses on strengthening the protection of personal information.

According to the Personal Information Protection Law, the people's procuratorate, the consumer organization specified by the law and the organization determined by the national cyberspace administration may file a lawsuit with the people's court. Actually, it is the first time that China includes the protection of personal information within the scope of public interest litigation initiated by the people's procuratorate, which used to be a new field in public interest litigation of people's procuratorate, and it was still at the pilot stage of continuous exploration. In September 2020, the Supreme People's Procuratorate issued the Guiding Opinions on Actively and Steadily Expanding the Scope of Procuratorial Public Interest Litigation Cases as the focus of case handling in the field of cyber infringement.

The Opinions pointed out that proactively and steadily advancing public interest litigation in procuratorate, establishing an information sharing mechanism for procuratorial public interest litigation and administrative law enforcement, and strengthen the handling of public interest litigation cases in key areas such as ecological environment and resource protection, food and drug safety, state-owned property protection, state-owned land use rights, protection of the rights of heroes, and protection of minors, and also Actively and steadily expanding the scope of public

²² The Shenzhen Chief Data Officer System Pilot Implementation Plan has already clarified 10 specific tasks in 3 areas, which involves the establishment of a chief data officer's working mechanism; includes the establishment of a chief data officer and introducing professional talents; clarifies the scope of the chief data officer's responsibilities including promoting the construction of smart cities and digital governments, improves data standardization management, promoting data fusion innovative applications, and implements normalized guidance and supervision. At the same time, the plan points out that it is necessary to strengthen the construction of the talent team and carry out the application and exploration of characteristic data; the development of the chief data officer evaluation and summary includes the establishment of the chief data officer evaluation mechanism and strengthening of work summary, etc.

interest litigation cases, exploring the handling of public interest damage cases in areas such as production safety, public health, protection of the rights and interests of women and persons with disabilities, personal information protection, cultural relics and cultural heritage protection, summarize practical experience, and improve relevant legislation.²³ The Personal Information Protection Law formally establishes the procuratorial public interest litigation system on personal information protection, which can further standardize the handling of relevant public interest litigation cases by the people's procuratorate and give play to the legal supervision function, effectively promoting the legal protection of citizens' personal information rights and interests.

In fact, relevant cases of personal information protection public interest litigation have appeared in Chinese judicial practice. In April 2021, the Supreme People's Procuratorate issued the Typical Cases of Public Interest Litigation on Personal Information Protection by Procuratorial Organs, involving 11 cases involving Internet companies collecting personal information in violation of laws and regulations and conducting consumer fraud, effectively supervising the field of personal information protection that seriously damages the rights and interests of personal information. The activities promoted the implementation of the main responsibility of the enterprise, and made useful explorations for the public interest litigation of personal information protection.

2.2. Two characteristics of Chinese Personal Information Protection Law

2.2.1. Modernity

As network information technology undergoes rapid development, personal information protection is increasingly valued by countries and regions around the world, and legislative activities related to it are also in full swing. According to official data released by the United Nations, 128 countries have enacted data protection laws, personal information protection laws, or data privacy laws, accounting for 69%.²⁴

The release of Chinese Personal Information Protection Law is a response to the personal information protection issues raised in the current era at the legal system level, providing legal solutions to strengthen the personal information protection. As well, it helps introduce Chinese experience and Chinese solutions to the problems of personal information protection commonly faced by countries all over the world.²⁵ Notably, the Personal Information Protection Law has

responded positively to issues such as face recognition, artificial intelligence and other new technologies that have been widely concerned by Chinese society in recent years. Plus, it touches upon the situation of big data-enabled price discrimination against existing customers and other issues, with distinct characteristics of the times. In response to the frequent abuse of face recognition in practice, Chinese Personal Information Protection Law also made a positive response. Article 62 of the Personal Information Protection Law stipulates: "The National Cyberspace Administration shall coordinate relevant departments to promote the following personal information protection work in accordance with this Law: (1) Formulate specific rules and standards for personal information protection; (2) Target small personal information processors, processing sensitive personal information and new technologies and applications such as face recognition and artificial intelligence, and formulating special personal information protection rules and standards..." This article sets out principles for the use of face recognition technology, and provides a basis for the relevant legislation to fine-tune the rules of face recognition technology.²⁶

In addition, since most countries in the world have entered the digital information society, the problem of cross-border transmission of information will inevitably arise. Chinese Personal Information Protection Law keeps up with the trend of the times and clearly stipulates China's personal information export system from the legal level, which solves the current legislative lack of rules for the cross-border transmission of personal information. Article 38 of the Personal Information Protection Law stipulates four statutory circumstances for the export of personal information: (1) Security assessment organized by the national cyberspace administration; (2) Personal information protection certification by a professional organization; (3) A contract has been concluded with the overseas recipient in accordance with the standard contract formulated by the national cyberspace administration, agreeing on the rights and obligations of both parties; (4) Other conditions provided in laws or administrative regulations or by the national cyberspace administration. The notification obligation of the personal information processor is also specified in detail, and individual separate consent is required. Providing personal information abroad is also a statutory matter that requires prior risk assessment. At the same time, it is required that operators of critical information infrastructures and personal information processors who process personal information up to

²³ See: *Supreme People's Procuratorate*. Requirements of the Central Committee of the Communist Party of China: Actively and steadily expanding the scope of public interest litigation cases. https://www.spp.gov.cn/spp/zd gz/202108/t20210812_526499.shtml, Last visit date December 2, 2021.

²⁴ URL: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>. last visit date December 23, 2021.

²⁵ See Wang-Liming & Ding-Xiaodong. Op. cit. P. 11.

²⁶ See Wang-Liming & Ding-Xiaodong. Op. cit. P. 14.

the number prescribed by the national cyberspace administration should be stored locally. It can be seen that the Personal Information Protection Law establishes the basic rules for the export of Chinese personal information through two aspects of transmission path and obligatory regulations, and does not adopt the "sufficiency protection" standard of the EU GDPR. Chinese Personal Information Protection Law does not adopt the EU GDPR "sufficiency protection" standard and set higher barriers to the circulation of personal information out of the country, but on the basis of strictly regulating the obligations of cross-border information providers, paying more attention to the use of market autonomy tools such as certification and contracts on the cross-border transmission of personal information, which is fully in line with the legislative purpose of promoting the cross-border flow of personal data followed by the international community.²⁷

2.2.3. Locality

The personal information protection systems are established in various countries in the world. On the one hand, the information subject is given the right to inquire, copy, delete, and correct. On the other hand, it imposes responsibilities on information processors to drive them to fulfill their obligations in terms of storage, information security, information quality, etc.²⁸

Chinese Personal Information Protection Law also follows this tradition and shows similarity to the widely used personal information protection system. In addition, Chinese legislators have fully considered China's basic national conditions during the legislative process, reflecting Chinese characteristics, like protecting the personal information of minors through the processing rules of sensitive personal information. Although GDPR also stipulates sensitive

personal data, it does not include information about minors, while Virginia Consumer Data Protection Act defines data involving children as sensitive personal data.²⁹

On the basis of fully absorbing the legislative experience of other countries, China has expanded the protection of sensitive personal information from children to minors under the age of 14, which is consistent with Chinese Civil Code, rendering the regulations on the protection of minors' personal information more specific and clearer. To illustrate further, there are two ways to set up personal information protection supervision in the world. One is the unified supervision model represented by the European Union, that is, the establishment of a special information protection agency to implement centralized supervision of all areas including public institutions and private institutions. The other is carried out by various functional departments to supervise activities according to their authority, and the protection of personal information is only part of their supervision responsibilities.³⁰

China has adopted the second model instead of establishing a completely independent personal information supervisory agency. The national cyberspace administration is responsible for the overall coordination of personal information protection work and related supervision and management, and performs relevant personal information protection duties, which depends on the high degree of professionalism of the national cyberspace administration. Judging from Chinese practical experience, the national cyberspace administration can assume the responsibility of overseeing personal information protection and to give full play to the various functions of regulatory agencies in law popularization, law enforcement, and propaganda.

²⁷ See *Zhang-Jihong*. Op. cit. P. 52.

²⁸ See *Wang-Liming & Ding-Xiaodong*. Op. cit. P. 11.

²⁹ See *Wang-Liming & Ding-Xiaodong*. Op. cit. P. 12.

³⁰ See *Zhang-Jihong*. Op. cit. P. 52.