Personal Data Protection from the Perspective of Public-Private Partnership

Shi Mingyu[1,a,*]

[1]*Law School, Peking University, No.5 Yiheyuan Road Haidian District, Beijing, China*
a. smyloveyj@sina.com
**corresponding author*

Keywords: personal data protection, public-private partnership, multiple values, compound right attributes

Abstract: Since the personal data protection involves lots of subjects, it has attracted people's attention both at home and abroad. Based on the compound attribute of personal data rights, different countries have taken different attitudes and measures concerning personal data protection from the perspective of Public-private Partnership. Through sorting out the current laws and regulations of personal data protection in China, it could be told that an imbalance still exists between the public laws and private laws in this field domestically. When entering into the new era, China can learn from the legislation mode of EU's GDPR and US's CCPA, break through the traditional mode and adopt various methods to protect the multiple values of personal data.

1. Introduction

At the end of 2017, Alipay launched the annual bill review function for the first time, which caused a heated response, leading many people positively shared their own bill on social platforms. However, a serious vulnerability was soon revealed that many users unconsciously authorizing the "service agreement" as Alipay on purpose utilized small fonts, the color resembling the background and acquiescence consent to confuse users. In the agreement mentioned above, there were terms allowing Alipay to analyze the personal data of the users and subsequently share the data together with the analysis results with any collaborate organization or partner institution. Yue Shenshan, partner of Yuecheng law firm, pointed out that according to *the Law on the Protection of Consumers' Rights and Interests*, users have their individual rights to make choices whether to accept the terms and conditions which should not be violated by Alipay. After more news media reported on the situation, the Network Security Coordination Bureau of the state Internet Data Office interviewed the people responsible for Alipay, accusing Alipay of breaching the terms of the Personal data Protection Proposal signed not long ago, and asked them to be held accountable for such situation. As a consequence, Alipay carried out immediate rectification in accordance with the correction proposal given by the Office.

Nowadays, as the science and technology develop rapidly, business models are changing with each passing day as well as the social issues, therefore, new era of Internet privacy crisis may arise

at any time. This paper focuses on how to break through the traditional model of protecting personal data and make a balance between personal data protection and modern society developing demand.

2. Problems in Personal Data Protection

2.1. Disputes on the Right Limit between the Subjects of Private Law

2.1.1. Right Disputes on Data Collection

When it comes to the data collection, it represents the process that the platform collects and stores the user's name, phone number, ID card number as well as other data when the user registers to use the product developed by the enterprise. During this process, based on the requirements of *Cyber security Law* and other relevant regulations, the platform is supposed to take the user's "informed consent" as the legitimate basis for collecting and using their personal data. Therefore, the platform tends to ask users to sign the privacy agreement before using the product. As mentioned above in the Alipay annual bill event, it reminds us of the dispute of rights between users and enterprises. On one hand, from the perspective of the enterprise, users' personal data turns out to be valuable, so the privacy agreement tends to contain a large number of standard clauses, which require users to authorize the collection and the use of personal data. As a result, it will bring risks to the subsequent improper use of personal data. On the other hand, from the perspective of the users, as data producers, although they are willing to authorize part of their personal data to the platform to receive more convenient services on the premise of privacy protection, as a matter of fact, they merely voluntarily transfer part of the ownership of their personal data. In practice, users tend to have no choice but to accept all the terms, thus losing the supervision and control of the data's subsequent use.

2.1.2. Right Disputes on Using Data

Data utilization refers to the processing of data after the enterprise has collected enough user data, which works to generate economic value. After processing the data, the enterprises will further share it with others, thus resulting in the data processor and the data transferee. Data sharing serves as a significant mode and profit-making means between enterprises. Without it, enterprises will fail to use the data again, which leads to the developments in data industry become impossible. However, in practice, two disputes will occur. First, for users, they will lose their control over personal data after the initial authorization, and the data transferee works as the new collector of personal data. However, there is no direct agreement between the user and the transferee, which weakens the power of the agreement signed between the user and the initial enterprise. That is to say, the use of personal data could not be satisfying enough. Second, for enterprises, when processing and collecting data, the initial enterprise has spent their labor and wisdom, therefore, in their eyes, they have certain rights to the processed data. However, due to the lack of laws and regulations, the specific rights between data processors and transferees are vague. In case of improper use, the responsibilities of both and relationship between them could not be told easily.

2.1.3. Right Disputes on Data Storage

The data storage is mainly divided into two stages. First, after collecting the data, the enterprise will automatically store it, thus offering corresponding services, as well as preparing for the subsequent processing. Since during this process, there are few rights disputes, it will not be discussed in this

paper. Second, it should be the storage of data after processing. The dispute focuses on the fact that the data at this time has certain added value, and whether the user is allowed to exercise the so-called "right to be forgotten" and ask the enterprise to delete his personal data. As the producers of data, users have the ownership of data. During the initial authorization, they use the data to exchange corresponding services, however, they do nothing but transfer part of the ownership. When they no longer need services, they have the right to withdraw the ownership and ask the enterprise to delete the data. However, after processing the data, enterprises have already spent their labor and wisdom, they are supposed to enjoy some derivative rights. That is to say, if individuals can ask enterprises to delete data at will, it will damage the interests of enterprises.

2.2. Differences of the Value Demand of Data in Public and Private Laws

On the whole, huge differences exist in the value demands and norms of public laws and private laws, and the personal data protection is of no exception. In this part, it will take the use and supervision of personal financial data as an example, thus studying the differences between the public and private value demand concerning personal data protection.

2.2.1. Data Utilization Is the Main Value Demand in the Field of Private Law

Based on the particularity of the financial industry, the personal data obtained by financial institutions when providing financial products or services for users is quite extensive. Besides the basic personal data such as name, ID card number, etc., it also includes personal property data such as family income, tax payment, all properties as well as investment risk preferences. Like what has been mentioned before, financial institutions will process the data after getting it and the data will be shared and comprehensively analyzed later between the financial groups, then institutions will launch targeted product recommendations and customer management based on it. This process is supposed to be one of the organizational advantages that the financial group pursues. Besides helping the institutions to reduce the cost of data collection and operation and realizing business expansion, it also offers them more comprehensive financial data of customers, reduces the operational risk as well as continuously enhances the financial competitiveness. Evidently, as the main body of private law, financial institutions take the use of personal financial data as their main value demand, so as to make more profits.

2.2.2. Data Protection is the Main Value Demand in the Field of Public Law

Driven by huge economic interests, quite lots of problems exist in the protection of personal financial data. For example, the disclosure of customer data due to the insecure data system and products; the staff of financial institutions use their power to illegally sell data; the financial institutions send marketing data to customers illegally for business, all of which have put forward higher requirements for the supervision of personal financial data.

The convenience of the accessibility of personal financial data also results that a large number of unqualified financial institutions compete disorderly, thus damaging the sustainable development of the industry. In this context, in order to regulate the financial market, the regulatory authorities led by the CSRC and the CBRC require financial institutions to protect customer data. Meanwhile, they began to supervise financial institutions. Since 2007, the Central Bank has agreed relevant files such as *Measures for the Storage and Management of Customer Identification*, *Customer Data and Transaction Records of Financial Institutions*, which gradually decide the collection scope and utilization principle of personal data. Later, there were other regulations and laws such as

Commercial Banking Law of China and *Measures of the People's Bank of China for the Protection of Rights and Interests of Financial Consumers*. As for the *Trial Measures for the Protection of Personal Financial Data*, it is also soliciting opinions, which reflects the main value demand of data protection in the field of public laws.

3. Analysis of the Right Attribute of Personal Data

As for the problem put forward in the first part, it is rooted in the obscure definition of the right attribute of personal data in legislation and real practice. In this part, it will analyze the right attribute of personal data.

3.1. Personality Rights

According to the theory of personality right, which supports the personality right attribute of personal data, which works to protect personality interests and is supported by some scholars. Professor Wang Liming holds that the personal data right has certain connotations, which is supposed to be a kind of personality right with independent significance. In the future personality right law of our country, the right of personal data is required to be stipulated as a separate personality right. According to Professor Qi Aimin, the release of *the General Rules of Civil Law* makes it clear that personal data should be protected as a legal interest. Moreover, in the future, the right of personal data should be established when compiling personality rights, so as to provide sources for specific personal data rights.

3.2. Property Rights

According to the theory of property rights, which supports the property right attribute of personal data, personal data embraces property interests, and the subject enjoys the right to regulate his personal data. The law should include personal data into the subject of property rights, thus applying certain laws to protect it. Professor Liu Deliang agrees with this view and believes that personal data property rights take the commercial value of personal data as the object's domination. To add up, professor Long Weiqiu also holds that a new data property rights system should be constructed.

3.3. A New Compound Right with Attributes of Personality Rights and Property Rights

Both theories mentioned above have their rationality. Comprehensively, personal data is equipped with dual attributes of personality and property rights. On one hand, the original personal data is able to directly or indirectly identify personal identity, thus reflecting personal dignity and free will. That is to say, it has the attributes of personality rights. On the other hand, due to the development of modern economy, personal data is not the data separated from each other, instead, it is the trading object with potential added value. Therefore, the processed personal data also has the property right attribute besides personality right. Professor Li Aijun agrees that personal data concerns personal interests, and valuable data should be the object of property rights. Since personal data involves personality and property rights, it is supposed to be complex speaking of the rights' attributes.

4. The Current Legislative Model of Personal Data Protection in China

Based on problems mentioned in the first part, adjustments should be made concerning the current

legislation. In China, personal data has been regulated in the field of private law and public law. Among them, significant provisions are sorted out as follows, so as to clarify the current legislative attitude and right protection mode of personal data protection in China.

4.1. Norms of Personal Data Protection in Civil Legislation

Table 1: Norms of personal data protection in civil legislation.

Law	Promulgation Time	Promulgator	Relevant Content
General Rules of the Civil Law	2017	National People's Congress	Article 111 The personal data of natural people is preserved by law. Any organization or individual that requires to get other's personal data should ensure its security according to law, and should not collect, use, process or transmit the personal data illegally, or illegally trade, provide or disclose it.
Cyber Security Law	2017	Standing Committee of the National People's Congress ("SCNPC")	Article 22 Any product or service online that has the function of collecting user data, the controller of which shall express and get consent from the user; when it comes to user personal data, it shall also abide by the provisions of this Law and relevant provisions on protecting personal data.
Law on the Protection of Consumer Rights and Interests	2013	SCNPC	Article 29 Operators and their staff must ensure the personal data collected from consumers strictly confidential and shall not illegally sell, disclose, or provide it to others. Business operators should adopt skills and other essential measures to ensure information security and prevent the disclosure and loss of consumers' personal data. In case of information disclosure or loss, remedies shall be taken immediately.
E-commerce Law	2018	SCNPC	Article 23 Where the relevant authorities require e-commerce operators to provide relevant data in accordance with the relevant provisions, the operators should follow the request. Relevant departments shall take necessary measures to protect the data and information security provided by operators, and keep strictly confidential the personal data.

4.2. Norms of Personal Data Protection in Criminal Legislation

Table 2: Norms of personal data protection in criminal legislation.

Law	Promulgation Time	Promulgator	Relevant Content
Amendment IX to the Criminal Law	2015	SCNPC	XVII. Article 253A of the Criminal Law is revised to read: " Whoever violates the relevant provisions of the state, sells or provides citizens' personal data to others, if it is of a serious nature, shall be sentenced to fixed-time imprisonment of not more than three years or criminal detention and shall be fined. "

4.3. Norms of Personal Data Protection in Administrative Legislation

Table 3: Norms of personal data protection in administrative legislation.

Law	Promulgation Time	Promulgator	Relevant Content
Regulations on the Disclosure of Government Information	2019	State Council	Article 15 The administrative agencies shall not disclose the government information involving business secrets, personal privacy and other public information that will damage the legitimate rights and interests of the third party.
Provisions on Protection of Personal data of Telecommunication and Internet Users	2013	Ministry of Industry and Information Technology	Article 9 When a telecommunication business operator or Internet information service provider collects or uses personal data of a user, he shall clearly inform the user of the purpose, method and scope, meanwhile, the channels for querying and correcting the information, and the consequences of refusing to provide the information, etc. shall be provided as well.

Based on the table above, it is evident that as for personal data, China focuses more on norms in the field of private law, less in the field of public law, and no special law has been formed in the administrative legislation. Meanwhile, no law has been formed to mention the right of personal data or data. Even according to Article 111 of *the General Rules of Civil Law*, it merely takes personal data as a legal interest rather than a legal right. That is to say, the current legislative model still needs to be improved.

5. New Methods for Personal Data Protection

5.1. Figure out the Main Responsibility of Personal Data Protection

Currently, scenes for the production of personal data have become more diversified. The generation, circulation and utilization of personal data turn out to be a continuous and interrelated process. In different stages, it involves different subjects and produces various responsibilities.

As a typical foreign data protection standard, *General Data Protection Regulation（GDPR）* has divided data subject into subject, controller, processor and recipient. According to this, the subject responsibility of personal data protection in China can be regulated as follows: when generating the data, as the data subject, users should strengthen their awareness of personal data protection. They should be careful about the authorization of personal data, avoiding general authorization, otherwise it will result in difficulties in later rights protection. When using the data, as controllers and processors of personal data, enterprises are required to follow the "informed consent" principle, obtain the authorization of customers in a legal and effective way, and make reasonable use of it. Moreover, they are not allowed to carry out other behaviors beyond their authority. In the subsequent storage of data, the controller, processor and recipient of personal data should offer citizens the "right to be forgotten" according to the real practice. When the user has stopped using their products or services, enterprises should stop collecting personal data immediately. Moreover, the user will be given the right to ask enterprises to delete or anonymously process their personal data. Certainly, during the whole process, the responsibility of regulators should not be ignored. As the main body of public law, with the aid of powerful regulations, regulators are supposed to ensure that the regulated enterprises use the data of natural persons according to legal procedures and authorized contents. Meanwhile, in pursuit of the efficient use of data, regulators should build an efficient data utilization mechanism as soon as possible.

5.2. Strengthen Public-Private Partnership to Realize Multi-Dimensional Value of Personal Data

The concept of public-private partnership should be traced back to the USA and the UK. In the United States, privatization and public private partnership are used to describe and define the cooperation between the public sector and the private sector. To be more specific, it should be "the formation of cooperative relationships between government, profit-making firms, and non-profit private organizations to fulfill a policy function". Considering that personal data has the compound attribute of personality rights and property rights, public and private partnership turns out to be necessary. Therefore, we should not only preserve the personality rights, but also collect and make full use of property rights. As for the personality rights attribute, due to the fact that compared with enterprises, individuals are in a weak position concerning data protection, it is necessary to establish a comprehensive and effective supervision mechanism with public laws, thus preventing the enterprises from abusing personal data and damaging personal interests. Speaking of the property right attribute, nowadays, with the continuous development of big data technology and the prosperity of data economy, as a significant data source, personal data is of great meaning to the development of enterprises and even the whole social economy. In order to encourage individuals to actively provide data, as well as encourage enterprises to collect and process data, the intervention of public law subjects is necessary as well, for they will build an effective data property right mechanism and system.

If we merely emphasize the property right attribute of data and the economic value of data,

personal data will become nothing but traded goods, which will weaken the public's sense of social security. If we put a strong emphasis on the personality right attribute of data, it will discourage enterprises to collect and utilize data, which is not conducive to economic development. Therefore, under no occasion should we separate the two. Instead, we are required to strike a balance between the two. That is to say, we should not only protect personal data, but also protect economic interests. In pursuit of this goal, it is suggested to form an effective supervision mechanism by public laws. Meanwhile, the active cooperation of the judicial subject is indispensable as well. Through the joint efforts, it will realize the effective protection and efficient use of personal data.

5.3. Establish the Legislation System of Personal Data Protection Comprehensively

According to the above analysis, the personal data legislation system in China is still insufficient and improvements should be made, thus forming a comprehensive personal data protection legislation system.

First, learning from the legislative experience of foreign countries is necessary. *GDPR* and *California Consumer Privacy Act (CCPA)*, as the representative extraterritorial data bills issued in recent years. Though belonging to the European Union and the United States respectively, they share similar legislative purposes, which are to strengthen the protection of personal data and privacy by regulating the behavior of enterprises in data processing. However, the positions and starting points of the two vary from each other. *GDPR* is based on the position of regulators, with the protection of basic human rights as the starting point, emphasizing the active regulations to process data carried out by relevant responsible subjects. However, as for *CCPA*, it is more inclined to consumers, focusing on regulating the commercial use of data. Viewed from the contents, *GDPR* stipulates that the use of personal data is "prohibited in principle and allowed when there is legal authorization", while *CCPA* is "allowed in principle and prohibited conditionally". At present, during the vigorous development of market economy in China, we should learn from *GDPR* to focus on the responsibility of the regulators. In the meanwhile, learning from *CCPA* is encouraged as well, during which we should pay attention to the commercial use of data and seek a balance of legislation in the end.

Second, from the perspective of the current situation of legislation domestically, in the current private law system, the right of personal data is not formally listed. Therefore, when revising *the General Rules of Civil Law* or issuing *the Civil Code*, we can take the right of personal data as a legal right. Meanwhile, due to that personal data has the attributes of personality right and property right at the same time, it should not be put into the title of personality right or the title of property right. Instead, it should be under a separate title which involves personal data right and other rights with complex characteristics. To add up, considering that in the current legislation system of personal data protection domestically, private laws account for a large proportion, while there are only regulations concerning the supervision in the administrative field. Therefore, we might as well set up relevant laws or reenact a more comprehensive administrative law. As the main body of public laws, government agencies should cooperate with each other, so as to promote the construction of a satisfying personal data protection system as well.

6. Conclusion

Nowadays, with the rapid development of economy, the value of personal data becomes diverse, thus resulting in the compound right attribute of personal data. Meanwhile, natural differences exist in the value needs of data between public laws and private laws. However, the utilization and

protection of personal data in China has not reached a balance concerning public-private partnership. Therefore, this paper works to study the legislative model and relevant experience of foreign countries, such as EU's *GDPR* and US's *CCPA* from the perspective of public-private partnership. Through this process, it hopes to break through the traditional protection of personal data. Moreover, it is suggested that while protecting the privacy of personal data, the commercial value should be fully tapped. Moreover, a personal data protection system with clear subject responsibility, public-private partnership and perfect laws and regulations should be established as soon as possible.

References

[1] *Paul M. Schwartz & Daniel J. Solove,Reconciling Personal Information in the United States and European Union,102 Calif. L. Rev. 877 (2014) .*

[2] *Wan Fang. Research on the principle of informing and obtaining consent and its alienation in the privacy policy[J]. Science of Law(Journal of Northwest University of Political Science and Law),2019, 037(002):61-68.*

[3] *Peiru Cai,Xinxi Wang. On personality protection and economic incentive mechanism in personal information protection[J].Journal of Comparative Law,2020(01):106-119.*

[4] *Fuping Gao. The Legal Basis of Processing of Personal Information——A Perspective of Interests Related to Personal Information[J].Journal of Comparative Law,2019(02):72-85.*

[5] *Liming Wang. Data sharing and personal information protection [J]Modern Law Science, 2019, 41(01):46-58.*

[6] *Wang Fang. The right to be forgotten——On the introduction of the right of forgetting in China[J]. Law Review, 2016(6):155-162.*

[7] *Jihong Zhang. On the legislative perfection of the protection of financial consumers' information right in China——Negative risk analysis of financial information flow based on big data Era[J].LegalForum, 2016(6) :92-1 02, 11 pages in total.*

[8] *Zhenhua Wu. Protection and utilization of personal information of financial consumers in the context of big data [J]Financial Technology Time, 2018, 280(12):53-56.*

[9] *Ding Luo. Research on the protection and supervision of personal financial information -- Based on the perspective of financial group business model [J]Journal of Contemporary Financial Research,2019(06):95-103.*

[10] *Liming Wang. On the legal protection of personal information right——Centering on the boundary between personal information right and privacy right [J]Modern Law Science, 2013(04):63-73.*

[11] *Aiming Qi,Zhe Zhang. Identification and re identification: definition of personal information and legislative choice [J]Journal of Chongqing University :Social Science Edition, 2018, 024(002):119-131.*

[12] *Deliang Liu. Property protection of personal information [J]Chinese Journal of Law, 2007(03):82-93.*

[13] *Weiqiu Long. Research on the construction and system of new data property right [J]Tribune of Political Science and Law, 2017(4).*

[14] *Aijun Li. Attributes and legal features of data rights [J].Oriental Law, 2018, No.63(03):66-76.*

[15] *Korab-Karpowicz W J . The united citizens organization: Public-private partnerships in global governance[J]. 2020.*

[16] *Lixiang Wu. The Application of Public-Private Partnership (PPP) in Judicial Trials. [J]. Southeast Academic Research, 2018, 000(006):170-180.*

[17] *Priscilla M. Regan,Legislating Privacy: Technology,Social Values and Public Policy (Chapel Hill,NC: University of North Carolina Press 1995) .*

[18] *Fuping Gao. Personal information protection: from personal control to social control [J]. Chinese Journal of Law2018,40(03):84-101.*

[19] *Weiqiu Long. On the path of property right of enterprise data protection [J].Oriental Law, 2018, No.63(03):52-65.*

[20] *Liming Wang. Civil code should strengthen the protection of personal information in data sharing [N]. BeiJing Daily,2019-02-18(010).*

[21] *Regulation (EU) 2016 /679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with re- gard to the processing of personal data and on the free movement of such data,and repealing Directive 95 /46 / EC (General Data Protec- tion Regulation) .*

[22] *Alan F. Westin,Privacy and Freedom 7 (New York: Atheneum 1967) ; Edward J. Janger & Paul M. Schwartz,The Gramm - Leach - Bliley Act,Information Privacy,and the Limits of Default Rules,86 Minn. L. Rev. 1219,1247 (2002) .*

[23] Xiao Cheng. Personal information protection from the perspective of civil code compilation [J]. China Legal Science, 2019, 000(004):26-43.
[24] George Christou, Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy, Palgrave Macmillan UK, 2016.
[25] Athur R. Miller, Personal Privacy in the Computer Age: The Challenge of New Technology in an Information-Oriented Society，67 Michgan Law Review, 1969.
[26] Paul M. Schwartz, Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Review, 2011.
[27] Paul M. Schwartz; Karl-Nikolaus Peifer, Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept, 98 Cal. L. Review, 2010.