Proceedings of the 2nd International Conference on Business and Policy Studies
DOI: 10.54254/2754-1169/7/20230204

Research on Personal Information Protection Legislation in the Digital Age: Based on the Comparison of Current Legislation in China, America and Europe

Wang Yi[1,a,*]

[1]*Zhejiang University City College, Zhejiang, China*
a. 915510596@qq.com
**corresponding author*

Abstract: With the development of Internet technology and the application of big data, the collection, dissemination and use of information become more convenient, people's private lives become more transparent, and concerns about information disclosure or illegal treatment of personal information also follow. By using the methods of literature analysis and comparative analysis, this paper tries to improve the legal protection mechanism of personal information in China by studying the latest legislation in Europe and the United States, and combining the national conditions and actual situation in China. Although the CCPA of the United States and the GDPR of the European Union have great reference significance, they should also pay attention to the potential problems existing in these two legislations, demonstrate the applicability of their practices with an objective and critical view, and formulate a personal information protection legal system with strong applicability that is suitable for China's national conditions.

Keywords: personal information, the right of informed consent, the right of information self-determination, the right to be forgotten, GDPR

1. Introduction

With the advent of the era of big data in 2012, it has become the scene label most closely related to the protection of personal information. The high-performance function of analyzing, processing and integrating fragmented information makes big data technology an intelligent lever to leverage the economic utility of personal information. Information aggregation mining, algorithm decision-making, user portrait, personalized recommendation are common in the digital society, accompanied by the abuse and disclosure of information. On a global scale, typical cases of improper use of personal information, such as "Cambridge Analysis" stealing Facebook user data to illegally manipulate political elections, "Dark Network" illegally trading information of Chinese hotel guests, Starwood guest reservation database being hacked, etc. [1], reflect the infringement of personal information ownership and information subject's right of informed consent by information collecting and using subject. Although in many cases, information subjects voluntarily provide their own information to the platforms or businesses based on their willingness to acquire goods or services, the subsequent use of the platforms and businesses does not strictly follow the principles and requirements for protecting personal information.

DOI: 10.54254/2754-1169/7/20230204

Take China as an example. Alipay's annual bill, which is widely concerned, illegally collects and uses the personal information of users. Alipay has various information about users' income, consumption, hobbies, life and so on. However, the default check of "I agree to Sesame Service Agreement" on the homepage entrance is undoubtedly a disguised way to collect user information, not to mention that the agreement almost unconditionally gives the user's personal information to a third party, and has the right not to support revoking the information inquiry authority of the third party.

According to the statistical report, as of December 2020, the number of Internet users in China reached 989 million. Among them, 38.3% of netizens suffered from network security incidents and "personal information leakage" was the hardest hit area of security incidents. It can be seen that the topic of personal information security and the protection of the rights of the subject of personal information has become an urgent focus of our attention. At the legal level, focusing on how to improve the existing legal system, explore a more reasonable law enforcement model, and how to protect citizens' personal information from a judicial perspective will become an important part of personal information protection in the new era.

2. Existing Problems

Personal information processing can be divided into information collection, information storage, information utilization, information sharing and circulation, and information deletion. Every link may infringe the rights of information subject [2]. Starting from the specific connotation of the right to personal information and combining with the "Alipay Annual Billing Event" mentioned above, we can summarize the characteristics of citizens' personal information impairment as consumers in the current economic activities from the following three aspects.

2.1. The Defects in Informing Behavior in the Personal Information Collection Link

In the "annual bill" incident, Alipay used an unspecified way to obtain the informed consent of the users who enabled this function, and did not use a way that would attract users' attention to obtain its authorization, which is essentially a violation of the right to informed consent. [3]. The scope of use and circulation of information collected in this way should also be limited. After undergoing interviews and rectification, Alipay cancelled the check of the default consent and adopted the method of mandatory reading of the informed consent notice, allowing users who do not agree to share data to use the service normally, while safeguarding the users' personal information security, and at the same time, ensuring their service experience to the maximum extent.

In reality, when collecting users' informed consent, a large number of platforms or websites use universal authorization instead of single authorization. The biggest problem with this method is that the one-time authorization of users will authorize their personal information to all subsequent sharing behaviors of the platform, which objectively poses a threats to the security of personal information.

2.2. Improper Application of Technology in the Use of Personal Information

With the continuous development of Internet technology, the global data volume has shown explosive growth. Data mining technology gathers data together, finds valuable information more quickly and accurately from massive, incomplete, noisy, fuzzy and random large-scale databases, makes inductive reasoning, excavates potential patterns, and helps people make correct decisions. Whether it is a reading website or a shopping website, the recommendation of the content that the user may be interested in is generated based on the analysis of the data such as the user's stay time on the browsing page and the browsing content. On the one hand, this greatly facilitates users to obtain convenient and quick personalized services. On the other hand, it exposes its privacy to some extent.

DOI: 10.54254/2754-1169/7/20230204

The 2016 Report on China's Personal Information Security and Privacy Protection pointed out that at present, citizens' personal information has been violated to a greater extent than widely expected. 81% of the people have received strange calls from the other people who know their personal information, such as their name or company. 53% of the people were constantly harassed by some kind of advertisements because of the disclosure of personal information after web search and browsing. As many as 36% of them have been harassed or cheated by marketing after their personal information such as renting, buying a houses, buying a cars, taking an exam, going to school and so on is leaked.

At present, China has extended this technology to the use of personal information, but the scope of application is only to protect the security of user account, which is a kind of precaution in advance. However, a large number of enterprises also use technology to make improper use of the information generated in the process of users' consumption, and the supervision on this phenomenon is still weak. In addition, there are businesses that track or even improperly crawl user data, and the post-event accountability mechanism for such behavior also needs to be improved.

2.3. The Storage and Deletion of Personal Information Lacks Perfect Specifications

In the Internet age, the behavior of storing and deleting personal information directly corresponds to the information subject's right of being forgotten. Whether this right can be fully guaranteed depends to a large extent on the will of the information storage subject and the degree of technological development.

On the one hand, information storage entities, mainly platforms or businesses, regard the personal information generated by users on the Internet and collected by them as important business assets, so in many cases, they do not want to permanently delete these data from their databases. Therefore, when users use it, they will find it easy to register an account, but difficult to log out.

On the other hand, with the rapid development of Internet data storage technology, some problems in the legal protection of personal information in our country are beginning to emerge. For example, online shopping consumption records, online mailing addresses, online comments and comments, which are typical examples of social software such as Weibo WeChat and Tik Tok. These information all reflect the trajectory of people's daily life. If people use data technology to steal improperly, the consequences will be unimaginable.

3. Causing Problems

3.1. Personal Information Involves Many Stakeholders

In the era of the Internet economy, with the addition of platforms, the main body of economic activities is more abundant than before. Different subjects have different interests in the collection, storage, use and circulation of personal information.

On the one hand, in addition to protecting personal privacy, consumers also have their own subjective will and are willing to provide their own private information to obtain ideal services. On the other hand, enterprises analyze the distribution of the target groups and their consumption preferences through the big data algorithm, so as to create greater profits, and they will also collect this information consciously. At the same time, however, in order to maintain a stable customer flow and enhance its corporate reputation, enterprises also need to take appropriate measures to protect users' personal information from being leaked. However, at present, the protection of personal information in China is still in the gray area, and consumers' self-protection awareness is weak, which is likely to cause many related problems.

DOI: 10.54254/2754-1169/7/20230204

3.2. High Risk of Technological Alienation

Based on the existence of commercial interests, enterprises are prone to misuse when they use technology to enhance their competitiveness. For example, they steal data by writing crawler programs, and over-collect data by compiling unreasonable algorithms, etc. Under the condition that the current standard is not perfect, it is easy to lose control. At present, China has promulgated the Personal Information Protection Law, which provides a clear legal basis for infringement of personal information. The enactment of the Law on Internet Security has made specific provisions for Internet crimes such as online fraud. However, due to the light punishment and high cost of safeguarding rights, victims generally do not choose to take legal actions to protect their legitimate rights and interests. In a word, although the laws and regulations of many departments have clear provisions on the protection of personal information, these laws and regulations are scattered. In the face of increasingly serious infringement of personal information, due to a series of factors such as difficult proof, high cost of rights protection, complicated procedures at the judicial level and so on, serious cases of infringement of personal information occur from time to time and become the biggest obstacle at the judicial level [4].

4. Suggestions

Personal information protection law, which originated from the social information transformation, has its unique characteristics. The research and development and application of new technologies not only give birth to a new economy, but also create new challenges. Countries represented by Europe and the United States began to examine the existing legal system, thus setting off a new wave of legislative amendments. Studying the legislative process at home and abroad and drawing useful experience is not only a change in line with international rules, but also a manifestation of responding to the needs of the times in light of national conditions.

4.1. Improve the Legislative Technology

Specifically, based on the principle of fair practice of information, the United States laid down the legislative purpose of personal information protection, adopted the legislative model of "separate legislation plus industry self-discipline", adjusted the legal relationship between individuals and public power in the form of separate legislation in the public domain, and restricted the legal behavior between private subjects in the form of industry norms in the commercial domain. Adhering to the legislative idea of personal information self-determination, the European Union brought personal information into the protection scope of personal rights, and formulates a comprehensive personal information protection law, which regulated both public and private fields, and comprehensively standardized the whole process of personal information processing[5]. What they are based on in common is to establish the institutional basis of legislation based on the national conditions and legal tradition, and at the same time, pay attention to the balance between the allocation of legal system and social and economic development.

In China, the scattered laws and regulations present typical behavior regulation characteristics. The construction of the code of conduct can be divided into three stages: information acquisition, use and possession. The corresponding standard system is set for each of the three stages. Any information acquisition, use and possession must comply with the requirements of the code of conduct, otherwise it will constitute "illegal" as stipulated by the law, and then go into practice with the aid of the implementation framework of the tort liability law. In the collection stage, the behavior of information processors to obtain personal information should be justified, reasonable and necessary. During the storage period, the information processor is entrusted with the security obligation to prevent information from being leaked or lost. In the development process, it is

DOI: 10.54254/2754-1169/7/20230204

prohibited to illegally process, transmit, sell or disclose personal information without personal consent.

The existing legislative practice can be divided into two models: the EU and the United States. The former unifies legislation to protect personal information as a basic human right, while the latter disperses legislation and is based on the right to privacy [6]. Although China has followed the example of the European Union and adopted a unified legislative model that is more suitable for its national conditions, there are still two problems. First, the types of responsibilities stipulated in the "Legal Responsibilities" chapter need to be clarified, and civil responsibilities, criminal responsibilities and administrative responsibilities need to be further divided, especially in the legislation, the boundaries of the three responsibilities need to be clarified and applicable rules need to be connected, so as to provide a legal premise for the development of learning and judgment, and enable the legitimate rights and interests of consumers to be implemented; Second, the penalties are not as strong as those imposed by the EU GDPR. The floating fine imposed by GDPR in EU is linked to the annual income of enterprises. In many cases, the punishment is not commensurate with the degree of law enforcement. In many cases, the penalties are not commensurate with the level of enforcement actions. It is not possible to effectively crack down on crimes against personal information.

4.2. Define Clear Criteria for Personal Information

Personal information, as its name implies, refers to all information related to a single natural person, including all information about facts, judgments, evaluations and other matters related to individuals such as the person's heart, body, identity and status. Personal information can be expressed in various forms, including graphics, audio and video, geographic information, transaction information, health status, social contact, etc. Even emotions can be digitized and quantified [7]. Because each country (region) has different social backgrounds in formulating relevant personal information protection laws, the specific definition of personal information varies from country to country. In the increasingly complex and frequently traded information age, the adoption of different definitions directly affects the boundaries of personal information protection. Generally speaking, there are three ways to define personal information, namely, generalization, "generalization+enumeration" and identification.

The general definition takes the EU as a typical example. Article 2(a) of the EU Personal Data Protection Directive (1995) stipulates: "Personal data refers to any information relating to a natural person that has been identified or can be identified". This definition is characterized by a high degree of abstraction and generalization, and has great advantages in application. However, if it is stipulated in a general terms, it will be "pocket-sized", which will inevitably lead to greater implementation cost in the practical application of laws.

The definition of "generalization+enumeration" absorbs the advantages of simple generalization, and at the same time, enumerates to make up for the difficulties of generalization definition in practical understanding. It has advantages. Taking Taiwan Province, China as an example, Article 2 of its Personal Data Protection Law stipulates: "Personal data refers to the name, date of birth, national identity card number, passport number, characteristics, fingerprints, marriage, family, education, occupation, medical records, medical care, genes, sex life, health examination, criminal record, contact information, financial situation, social activities and other data that can directly or indirectly identify the individual".

An "identifying type" is defined in a way that "identifies" an individual to define personal information. As long as the information can be associated with a specific person, or can confirm a specific person with the aid of information, it is considered as personal information [8]. Article 76 of China's "Network Security Law" issued in November 2016 stipulates: "Personal information refers

DOI: 10.54254/2754-1169/7/20230204

to various kinds of information recorded electronically or otherwise that can identify a natural person individually or in combination with other information, including but not limited to a natural person's name, date of birth, ID number, personal biometric information, address, telephone number, etc." From this, we can see that the definition method adopted in the "Network Security Law" is "generalization+enumeration" and the key word is "identifiable". The Personal Information Protection Law passed on August 20, 2021 gave a more condensed interpretation. Article 4 of the law stipulates that: "Personal information refers to all kinds of information relating to identified or identifiable natural persons recorded electronically or by other means, excluding anonymous information.

Therefore, in the definition of personal information in the personal information protection legislation, in order to maintain the coordination of legislation, we should adopt the same definition as above, that is, general or exemplary definition. Through the above analysis, the connotation of personal information can be summarized as the sum of the information that can be used alone or combined with other information to identify a specific individual, including but not limited to objective information about individuals, biological information, etc.

4.3. Clarify the Subject of Law Enforcement and Its Scope of Authority

China's relevant regulations on personal information protection are scattered in the criminal law, civil law, administrative law and other legislations. Different regulations and understandings have been made on the connotation of personal information, including privacy protection in the traditional sense and personal information protection in the context of big data. In the definition of the concept of personal information, there is a phenomenon of "The academic circle of criminal law finds criminal problems, and the field of civil law finds civil issues". In the judicial practice, the identification of "personal information" and "personal privacy" by the courts and administrative organs is ambiguous [9]. The direct consequence of this is unfavorable to the protection of personal information rights and interests. Just think, when a personal information infringement case occurs, the law enforcers of the criminal law department think that "it is not under the jurisdiction of the criminal law" and the law enforcers of the civil law department think that "it is not under the jurisdiction of the civil law". Then, if personal information does not fall within the scope of the department to which it belongs, what basis does the information subject have for seeking protection under the circumstance that the constitution of our country cannot be sued? As a matter of fact, it is in an unprotected state. In addition, the specific and detailed provisions on personal information protection are common in government regulations, and the legal rank is not high, which leads to the lack of authority in the enforcement of personal information protection and is not conducive to personal information protection.

The relevant provisions on the protection of personal information are distributed in nearly 270 legal documents. However, these legal documents do not clearly stipulate which procedures and measures should be taken by which authority to stop loss in time when personal information is infringed, which leads to the unclear situation of law enforcement agencies. In other words, the decentralized legislative provisions have led to the formation of "segmented" multi-head supervision over the enforcement of personal information protection [10], with each department performing its own duties. This can easily cause the law enforcement departments to pay attention to their own "statutory authority" in the law enforcement, and the phenomenon of "hopeless commons" will appear in the overlapping parts of various department. Another noteworthy situation is that for the overlapping part that are beneficial to the handling and management of cases by subordinate departments, the authority departments take the initiative to declare their powers. However, the authority department shirk responsibility for the overlapping part that belongs to their own

DOI: 10.54254/2754-1169/7/20230204

responsibility, which easily leads to inconsistent and unbalanced powers and responsibilities of law enforcement department.

5. Conclusion

Personal information, as an important strategic resource in the new era, has great significance. Based on different political and historical backgrounds and value orientations, each country or region has shaped different personal information protection models. Europe and the United States, as long-term leaders of personal information protection research, have provided overseas experience for our country's legislative work. Through the comparative research and analysis of GDPR and CCPA, combined with the current situation of personal information protection in our country, apart from changing the legislative model and clarifying the legislative standards, the focus is on how to regulate the behavior of law enforcement subjects, so as to provide all-round legal support for personal information protection. This study will lay a foundation for the internationalization of China's personal information protection legislation, provide a normative basis for the cross-border flow of data, effectively enhance the protection of personal information, and promote the orderly development of the information industry and society.

References

[1] *Li Meng. Personal information protection legislation [N]. Journal of xinxiang university, 2016 (02)*
[2] *Samuelson, "Is Information Property?", Communications of the ACM,vol.34,issue.3,(1991).*
[3] *Li Quntao, Gao Fuping. Information subject agreed to the applicable boundary [J]. Financial Law, 2022 (01)*
[4] *Liang Yan. Research Report on the Current Situation of Personal Information Protection in the Age of Big Data [J]. Legal System and Economy, 2020 (02)*
[5] *Barbra Vander Auwermrule, "How to attribute the right to data portability in Europe:A comparative analysis of legislations",Computer law & Security Review,(2017).*
[6] *Loir Jacob Strahilevitzf, "Reunifying Privacy Law", Califfornia Law Review,Vbl.98, No.6(2010)*
[7] *Michael L, Rustad & Thomas H. Koenig, "Towards A Global Data Privacy Standard", 71Fla.L.Rew.365,(2019).*
[8] *Chen Shipeng. Personal information protection legislation concept and model research [D]. Lanzhou University, 2019*
[9] *Diaz C, Tene O, Guerses SF,"Hero or Villain:The Data Controller in Privacy Law and Technologies",74(5)Social Science Electronic Publishing.937,(2013).*
[10] *Lu Liangcong. Personal information protection in the comparative perspective of .GDPR and CCPA [D]. Shandong University, (2020)*