ISSN 2616-5902 Vol. 3, Issue 8: 5-9, DOI: 10.25236/AJBM.2021.030802

Consumer Privacy Protection based on Data Subject Rights

Wei Wang, Mengjiao Zhou

Business School, Shandong m of Technology, Zibo, 255000,China

Abstract: *Based on the rights of data subjects, this paper concludes the problems existing in the privacy protection of consumers, and puts forward corresponding countermeasures and suggestions from the aspects of law, risk management and technology application.*

Keywords: *data subject, consumer privacy, GDPR*

1. Introduction

With the development of computer technology , the generation and storage of data are becoming more and more convenient. Various organizations have their own massive data sets. Business enterprises, banks, insurance companies and other service enterprises can make use of the acquired consumer data to process and analyze, grasp the characteristics and preferences of consumers through data, and design products and services that are more in line with the needs of consumers. The emergence of big data optimizes products and services, but on the other hand, the production and utilization of big data make it easier for consumers to obtain privacy data, and the problems of privacy security and protection become particularly prominent. On May 25, 2018, the general data protection regulation (GDPR) came into force [1]. The regulation is similar to the "safe harbor" agreement signed by the U.S. Department of Commerce and the European Union in December 2000, both for the protection of personal data when collected by third parties such as enterprises [2].

The data subject is "an identifiable natural person", that is, "an individual that can be identified directly or indirectly, especially through one or more physical, physiological, genetic, spiritual, economic, cultural or social identities unique to a natural person, such as name, identity number, address data, network identification or natural person" [4]. The data subject transforms various events or phenomena in the real physical world into data, and can also transform different information in the virtual data world into decisions and actions in the real physical world [3].

2. Rights of Data Subject

Internet technology enables each data subject to play its own value and is actively bringing new benefits to the society and the country. Each identity should have some corresponding rights, and the data subject is no exception. The EU GDPR stipulates the rights owned by the data subject and ensures that these rights are not infringed as much as possible.

Chapter III of the general data protection regulations stipulates seven basic rights owned by data subjects, and the specific concepts are shown in Table 1. The seven basic rights are the right to know, the right to access, the right to correct, the right to delete (the right to be forgotten), the right to restrict processing, the right to object and the right to carry data [3]. According to the nature and characteristics of rights, they can be divided into three categories: the first category is the right to maintain the dignity of the subject, including the right to know, the right to visit and the right to correct; The second category is the right to passively control the use of data, including the right to delete (the right to be forgotten), the right to restrict processing and the right to object; The third category: the right to actively control the use of data, including the right to carry data. Seven fundamental rights see table 1.

ISSN 2616-5902 Vol. 3, Issue 8: 5-9, DOI: 10.25236/AJBM.2021.030802

Table 1: Composition of data subject rights

Serial number	Data subject rights	Specify
1	right to know before	When personal data is collected, the data controller must provide the data subject with all the information he or she needs to know, including the controller's own information, in easy to understand language.
2	Access rights	Data subject has the right to know through the controller whether its personal data is being processed. If it is being processed, it has the right to access personal data and know all information related to its personal data processing.
3	Right of correction	When the personal data of the data subject is inaccurate or incomplete, it has the right to let the data controller modify its personal data
4	Right to delete (right to be forgotten)	Under certain circumstances, the data subject has the right to stop the data controller and third-party institutions from processing and deleting their personal data.
5	Restricted processing rights	Under specific circumstances, the data subject has the right to let the data controller restrict the relevant processing of personal data information.
6	Right of objection	Data subject has the right to object to the data processing of his personal data.
7	Data portability	Under certain circumstances, the data subject has the right to obtain relevant personal data sorted, widely used and machine-readable through the data controller, and has the right to transfer such data from one controller to another without obstacles.

3. Questions in consumer privacy risks based on RDS

Based on the seven basic rights of data subjects, consumer privacy risks and protection issues can be divided into five categories. algorithm technology infringes the right to know and access, restricts the conflict between processing rights and information freedom, corrects and deletes the right to destroy data integrity The "cocoon room effect" formed by derived data violates the provisions on the right of objection and the abuse of the right to carry data, resulting in unfair competition.

3.1 Computing technology infringes consumers' right to know and access

The development of computing technology has expanded the ability to obtain, process and use personal information. Decision making no longer depends on the intuition of managers, but on accurately recorded consumer behavior data [4]. Preferences are calculated and pushed according to consumer behavior data. In the process of receiving services, consumers do not know everything behind them, personal information is collected unconsciously, and consumers' right to know is violated. For example, big data algorithm discrimination. In recent years, the phenomenon of "big data ripening" has occurred frequently. For accounts with consumption records in Ctrip, the price of online booking the same room in the same hotel is significantly higher than that of accounts without consumption records; Consumers who use Didi platform book the same route, and users who use online car Hailing platform more frequently will have higher prices, and even consumer mobile phone brands will affect the predetermined price [5].

Data is the expression and representation of the world. The people who design the initial algorithm program may have some bias or even discrimination against some consumers. The bias or discrimination are expressed through the algorithm program and constantly consolidated. Algorithmic discrimination virtually infringes consumers' right to know and access.

3.2 Restrictions on processing rights conflict with freedom of information

Although consumers' personal privacy is very important, the expression and circulation of information is also very important. Restricting the processing right can allow the data controller to restrict the relevant processing of personal data information and protect consumers' personal data from being infringed arbitrarily; To exercise the two rights of freedom of expression and freedom of information, consumers may not be able to use the right to restrict processing.

The two rights of restricting processing power and freedom of information will conflict under certain circumstances, and they restrict and restrict each other. If data processing is restricted in order to protect consumers' privacy and rights, data circulation will undoubtedly be hindered, and social development and progress may be very slow. How to choose when there is a collision between consumers' limited processing power and information freedom is not only a problem worthy of thinking, but also an

ISSN 2616-5902 Vol. 3, Issue 8: 5-9, DOI: 10.25236/AJBM.2021.030802

inevitable problem with the rapid development of technology.

3.3 Correction and deletion rights destroy data integrity

The right of correction and forgetting owned by the data subject means that under specific circumstances, the data subject can allow the data controller or a third-party organization to modify or delete its personal data information. However, big data is characterized by "full sample". The calculation of incomplete data may lead to some deviation in the calculation results, which may further lead to wrong decisions. If a large number of data subjects exercise the right of correction and forgetting, delete and cover up personal key information, the value of incomplete data sets will be greatly reduced, and the analysis and decision-making based on incomplete data also have unpredictable risks.

On the other hand, the data value is not fully expressed through one-time analysis. The continuous analysis and mining of information processors may make the data value fully displayed and utilized. When a specific purpose is achieved, if the data subject data is deleted immediately, the data has not been fully mined, and its potential value cannot be reused.

The right to correct and be forgotten owned by the data subject does protect the privacy and security of consumers, but the deletion of personal data will destroy the integrity of data.

3.4 The "cocoon room effect" formed by the derived data violates the provisions on the right of objection

In the era of big data, data has gradually become an indispensable part of market competition. Data controllers and processors can capture, process and process it, so as to form derivative data with high market value.

According to the derived data information, we can easily locate the corresponding consumers by using "re identification" and other technologies, and carry out information collection, specific push, personalized pricing, etc. Many Internet companies push personalized data services for consumers. When consumers occasionally change the information topic which they pay attention to, the intelligent algorithm will push again according to the new information topic. In this way, consumers passively accept the same type of information every day. Unless they actively choose, they can contact different types of information. "Information cocoon room" makes consumers' views gradually one-sided, one-sided views will gradually increase, and even take some biased views as truth and misjudge things.

3.5 The abuse of data portability leads to unfair competition

The data portability right stipulates that under specific circumstances, the data subject can transmit personal data information, so as to promote the flow and dissemination of information. By promoting data flow, encourage effective competition between enterprise platforms and reduce the locking effect of a single platform on user data. Registered user information has become an important business resource in the hands of Internet operators. In order to obtain more user information, some enterprises use large platforms to capture user information and intercept competitive resources, resulting in unfair competition among enterprises, and consumer information has not been effectively protected. For example, in the "first case of Internet anti unfair competition", pulse illegally captured and used the user information of sina Weibo, intercepting the competitive advantage of sina Weibo without justification.

Protecting all kinds of user information on social network platforms is not only a necessary condition for Internet operators to carry out normal business activities, maintain and improve user activity and maintain competitive advantage, but also a respect and guarantee for the rights and interests of users. When cooperating with the social media network platform, other operators should not only legally obtain the user information of the social network platform, but also properly protect and properly use the user information.

4. Countermeasures and suggestions

4.1 Continuously improve the legal system of consumer privacy protection

China's legal system on consumer privacy protection is not perfect. The legal protection of personal privacy is mainly based on some items in relevant laws such as civil law, constitution, tort liability law

ISSN 2616-5902 Vol. 3, Issue 8: 5-9, DOI: 10.25236/AJBM.2021.030802

and criminal law. The independent legal status of the right to privacy in judicial practice must be established through legislative procedures, Accelerate the progress, study and formulate legal norms to safeguard consumers' privacy rights and interests, and make clear provisions in the following three aspects in the form of law on the security of consumers' privacy.

First, the dynamic processing of data clearly distinguishes different protected objects. When processing different data, we should focus on the direction to realize the appropriate and necessary criminal law provisions, comprehensively protect the storage and use of personal data, provide access rights, correction rights and forgotten data subject rights for protected objects, and introduce responsibility mode from the scope of application, data protection principles Establish the legal framework of personal data protection in terms of the legitimacy basis of data processing, the rights of data subjects, the obligations of controllers and processors; Second, accelerate the research and formulation of laws and regulations to safeguard consumers' privacy, and make clear provisions in the form of legal provisions in combination with China's specific legal environment; Third, formulate special open sharing measures and scientific data management, standardize the processing and open sharing of personal data in detail, and clarify the data rights of data subjects on their personal data, such as the right to know, access, correction, deletion, restriction of processing, data portability, objection and so on.

4.2 Using technical isolation to avoid data incompleteness

At present, with the development of information technology, consumers' control over personal privacy is becoming weaker and weaker. In many shopping environments, anonymity is not allowed or impossible. While developing information technology, we should also pay attention to and strengthen the development of consumer information security protection technology. For example, disrupting consumers' data, deleting unique identifiers, encrypting consumers' information, etc., so as to make users' information fuzzy, which can prevent criminals from using consumers' data information to identify consumers, and play a certain role in protecting consumers' privacy and security.

However, the current data integration technology can recover the fuzzy processed data, obtain complete data information and identify individuals. Therefore, the full cycle security area required for source code storage, circulation and use can be constructed through multiple isolation technical means such as disk, storage, peripherals, network and application, so as to realize data technical isolation. Technical isolation can isolate data information from the mass world, and the data information remains intact. This can not only protect consumers' information from being easily obtained, but also protect consumers' privacy. Consumer data information can be reused under necessary conditions.

4.3 Using blockchain technology to encrypt consumer derived data information

Consumers' personal data information is closely related to economic interests. If consumers' identity information, use records, transaction records and other sensitive information are maliciously obtained by criminals, it will have a great impact on consumers.

There are risks to consumers' privacy security, most of which are due to the theft, dissemination and utilization of consumers' data information. As an emerging technology, blockchain can solve the digital management permission problem of user privacy protection.

Blockchain can realize low overhead, protect consumers' derived data information, encrypt and manage all consumers' information by using blockchain technology, enable consumers to have their own information management authority and protect consumers' privacy and security.

In addition, each node of the blockchain can store complete data. Using blockchain technology, users can view the data on the blockchain at any time, which can well realize the openness and transparency of data information. Moreover, in the blockchain, if one of the blocks is to be modified, all the subsequent blocks must be recalculated. The modification of a single node cannot effectively modify the data. Therefore, digital rights management based on blockchain technology can prevent transaction information from being tampered with. After the consumer's derivative data information is encrypted by blockchain, the consumer's derivative data information is hidden in the Internet. At the same time, consumers can view their personal information usage openly and transparently, and consumers will not have privacy disclosure in the process of applying for information encryption. Using blockchain technology to encrypt consumers' derived data information can effectively protect consumers' privacy and avoid the formation of "cocoon room effect".

ISSN 2616-5902 Vol. 3, Issue 8: 5-9, DOI: 10.25236/AJBM.2021.030802

4.4 Strengthen the risk management of personal data in open data sharing

According to the research on EU GDPR and personal data protection at home and abroad in recent years, it is found that the protection of personal data related to research science or history by GDPR is also applicable to the open sharing of scientific data. The personal information contained in scientific data is the same as the personal information contained by consumers based on the rights of data subjects. Information privacy and security are facing great risks and need more strict data risk management.

Chapter IV of the EU GDPR stipulates the responsibilities of data controllers and processors, including the general responsibilities of data controllers and processors, the responsibilities and measures of data controllers and processors for personal data security, and the evaluation of the impact of data protection. When consumers' personal data is open shared, data controllers and processors have different ways to deal with personal data information, which may bring different risks to consumers' privacy and security. Data controllers and processors actively predict the risks in personal data, which can well identify and deal with the risks, so as to better protect consumers' rights and privacy.

5. Summary

The research on consumer privacy risk and protection based on data subject rights is an issue that cannot be ignored in the era of big data. Focusing on the research on consumer privacy risk and protection based on data subject rights, this paper makes a detailed analysis on the legal system, technology development and risk management from the seven basic rights of data subjects, The corresponding countermeasures are given. Under the condition that the protection of the rights of data subjects is strengthened, the problem of consumer privacy risk is also reduced accordingly. Even so, there are still many problems to be solved in consumer privacy protection.

Acknowledgments

This work was financially supported by fund 9010-513014: Privacy protection in medical information integration and mining.

References

[1] Ding Xiaodong. What is data rights—— Protection of data privacy from European general data protection regulations [J]. Journal of East China University of political science and law, 2018,21 (04): 39-53.
[2] Zhao Cen, Li mengran, Jin RiFeng. Thoughts on privacy in the era of big data [J]. Science Bulletin, 2015,60 (z1): 450-452.
[3] Tian Guanglan. Data subject rights and their pending issues in the era of big data -- Taking the EU general data protection regulations as the analysis object [J]. Journal of Renmin University of China, 2020,34 (06): 131-141.
[4] Tianqi Zhang. Law on Personal Data Protection in the Age of Artificial Intelligence[J]. International Journal of Social Science and Education Research,2021,4(5).411-421.
[5] Li Dan. Algorithm discrimination against consumers: behavior mechanism, profit and loss definition and collaborative regulation [J]. Journal of Shanghai University of Finance and economics, 2021,23 (02): 17-33.