

Research on the Legal Protection of Personal Information Security in the Era of Big Data

Xu Wei¹, Nie Yi²

¹Department of Information Technology, Hubei University of Police, Hubei, China, 430034

¹Hubei Cooperative Innovation Center for Electronic Data Forensics, Wuhan, Hubei, China, 430034

²Law Department of Hubei University of Police, Wuhan, Hubei, China, 430034

Keywords: personal information; legal protection; era of big data

Abstract: In the information society, technological progress has promoted the development and use of personal information, but also exposes personal information to the great risk of being leaked and misused. How to strengthen the protection of personal information security is a problem that needs to be solved urgently in terms of social development and technological progress. This paper describes the relationship between big data and personal information security, analyzes the problems and causes of personal information protection under big data, and provides measures to strengthen the protection of personal information during big data operations.

1. Introduction

Personal information security is an important field in the subject of information security. As a comprehensive subject, information security includes many aspects, such as computer science, information science, information security and so on [1]. The contents of information security include system security, computer operation security and information security. In the process of storage, dissemination, sharing and use, personal information is in a state of secrecy, security, integrity and control, so that personal information is not subject to external threats and internal interference is an important content of personal information security. Personal information security is closely related to personal life, in the era of big data, strengthening the protection of personal information security can effectively protect citizens' right to information, ensure tranquility, reduce crime, and protect personal safety. Therefore, the protection of personal information security must be strengthened to ensure the stability of everyone's life.

2. The New Challenge of Personal Information Security under the Background of Big Data

2.1 Multi-party interests in personal information

Information technology has made the collection of personal information intensive, and the depth and breadth of personal information processing and utilization have also greatly increased. The main body of information is the direct beneficiary of the development of personal information value. People's daily lives such as social networking, shopping, transportation, entertainment, medical care, and insurance are becoming more convenient and smart, and the price they pay is that personal information is illegally collected and abused. Technological advances have greatly weakened the ability of information subjects to control and dominate personal information. Under the dual influence of the continuous awakening of individual rights consciousness and the increasingly widespread use of personal information, the desire of individuals as information subjects to strengthen the protection of personal information security becomes more and more urgent. With the support of big data and related technologies, the channels and scope for collecting personal information by commercial organizations have been greatly expanded, the accumulation of personal information has exploded, and personal information analysis and mining capabilities have greatly increased. The commercial value of personal information has stimulated a strong demand for

commercial organizations to collect and use personal information. And the necessity and justification of the development and use of personal information by business organizations are gradually accepted by society.

Collecting and processing personal information for public management purposes is a common practice among governments. In the context of big data, the personal information collected by the government is larger in size and broader in scope, and the ability to integrate and analyze personal information is also stronger. The new generation of information technology has strengthened the social value of personal information, especially in the fields of public policy and public safety. From a more macroscopic point of view, informationization is an inevitable result of social development. Government is the largest collection and user of personal information and it is also the protector of personal information. Government should ensure the security of personal information during the development and use of personal information, urge the relevant organizations and individuals to legally collect and use personal information, and maintain the basic rights of information subjects. Therefore, government also has the dual status of personal information users and protectors.

2.2 Conflicts of interest on personal information

In the era of big data, the idea of protecting the personal information and the fully developing and utilizing of personal information have been deeply rooted in the people's mind, so that the contradiction between the protection and utilization of personal information is more prominent and complicated. On the one hand, strengthening the protection of personal information to maintain the personal dignity of the information subject is bound to limit the collection and utilization of personal information to a certain extent, thereby reducing the economic value of the corresponding personal information, hindering the development of the social economy and reducing the overall welfare level of the society. On the other hand, strengthening the development and utilization of personal information will inevitably increase the possibility of personal information being touched by others, thus increasing the possibility of the corresponding tort. If the basic rights of the information subject are not protected, the enthusiasm for providing personal information will be frustrated, leading to the choice between refusing to provide or providing false information. The accuracy of personal information cannot be guaranteed, and the value of personal information development is impossible. If the conflict of interests between the protection and use of personal information is not properly solved, it is inevitable that the security of personal information will not be effectively guaranteed, and the development and utilization of personal information will be also in difficulty.

3. Problems and Causes of Personal Information Security Protection in Big Data Operation

3.1 Problems

The laws and regulations that China has promulgated have focused on the protection of personal information data mainly in the formulation of principled opinions, and have not explicitly provided specific protection measures for personal information data. Therefore, the government has not introduced laws specifically protecting personal information, resulting in the lack of targeted protection of personal information [2]. The industries involved in relevant administrative regulations are usually the search engine industry and the communication industry, ignoring the vast number of social platforms, page-side registered online games, and huge e-commerce industry. In addition, existing administrative regulations cannot enumerate all kinds of ways of infringing on personal information on the Internet, which shows that the development and changes of big data technology have left behind the static laws and regulations.

The large-scale operation of big data has led to the gradual reduction of the cost of infringing on personal information, followed by the protection of personal data and information. Business organizations must defend internal information disclosure, third-party malware, and hackers through the most advanced procedural technologies. As commercial institutions reserve a large number of consumer personal information data, while resisting external infringement of consumer personal information data, it also requires that commercial institutions have strong self-discipline and do not

touch the following two infringements. Firstly, they should not overanalyze all the data in the database and obtain the privacy information for all the data in the database because of the economic benefits. Secondly, businesses cannot discard information security because of high security-related obligations leading to high commercial costs. This not only requires the high self-discipline of commercial organizations in the Internet sector, but also requires the government to take the lead in establishing a strong monitoring agency.

3.2 Causes

In the era of paper media, the way of collecting data is relatively simple. The behavior of infringement of the right of privacy and reputation through citizen's personal information data is basically one-to-one pattern, and the scale of crime is in a small scope. The emergence of cloud storage technology is accompanied by the mutual access of the global network, which makes the user's personal information bound into a database, making the form of one to one infringement rapidly into one-to-many or even many-to-many forms of infringement. The operation of large data itself accelerates the speed of information circulation and the overall scale, with the enlargement and diversification of the netizens, which leads to a sudden change in the way of infringing the rights and interests of the users.

Because the whole process of big data is completed through computer server and cloud computing technology, human traces are very vague [3]. First, the over-analysis of big data is cryptic. The data control center utilizes a self-built database or connects multiple databases, accesses the Internet, adopts various programming language frameworks, and taps other people's information associated with user's personal information, thereby interpreting all the marks left by users in the Internet space. In this process, people only need to set up the relevant computer program and test it through the server. All other processes are analyzed by the data processing terminal itself. In the excessive resolution of personal information, the degree of human participation is very low and the transparency is very poor, which fully shows the concealment of the overanalyzes process.

4. Countermeasures to Perfect the Legal Protection of Personal Information Security in China

4.1 Clear the basic concept of legal protection of personal information

The basic legal aspects of human information protection, such as the scope of personal information, the rights attributes and specific content of personal information rights, must be clearly defined through corresponding legal provisions, and lay the right basis for the protection of personal information. First of all, it should clarify the scope of personal information. Since the development of information technology obscures the identification boundary of personal information, the scope of personal information should be limited from the identification of the consequences of recognition. Secondly, we must clarify the nature and content of personal information rights. The specific personality right of personal information rights must be established in the Basic Law for the Protection of Personal Information, and the contents of the personal information rights system must be comprehensively and specifically described.

4.2 Carry out classified protection of personal information

In view of the conflict of interests between personal information protection and personal information development and utilization, to better realize the balance between them, it should be classified according to the different nature of personal information in law. Specifically, it is suggested to divide personal information into two kinds: sensitive information and non sensitive information in the personal information protection law. Sensitive information includes personal information of special subjects and important areas, and the law should strengthen its protection. In addition to the limited use of national institutions for the purpose of maintaining public order and national security, it is prohibited to collect and use any operating institution before it has received personal consent [4]. Non-sensitive information refers to corresponding information that does not involve personal privacy, for such information, the law should not only allow state agencies to use for the purpose of

performing functions, but also encourage operators to adopt various legal methods for collection and use, thus giving full play to the role of personal information in promoting the economic development in the era of big data.

4.3 Clear the rights and obligations of information managers

In the era of big data, the main body for collecting, using, and processing personal information is not the individual citizen who has the personal information rights, but the enterprise or the corresponding government agency that serves as the information manager. Therefore, information managers have very important significance for the legal protection of personal information. Because of the importance of personal information for business activities and social management, the law should clarify the right of the information management company or official organization to use related personal information. At the same time, in order to properly protect personal information in the process of collecting, using, and processing corresponding personal information, it is necessary to set appropriate rights and obligations for the information managers.

4.4 Strengthen the supervision of law enforcement

The protection of personal information is a kind of dynamic process, that is, the right of information subject is not infringed in the process of collecting and using personal information. The realization of dynamic security depends on the effective implementation of the information protection law. Strengthening the supervision of personal information processing and utilization activities is a way to balance the protection and development of personal information. Set up special personal information protection agency to ensure the management of personal information and users to fulfill their information security protection obligations. And we should strengthen supervision over the use of personal information, and urge personal information managers to constantly improve their technological level and risk awareness so as to enhance personal information security.

5. Summary

In the context of big data, the value of personal information has become increasingly prominent. The development and utilization of personal information has become a trend. The development and utilization of personal information can promote industrial development and enhance social welfare, but it will also pose a serious threat to personal information security. Therefore, it needs to seek a balance between the protection of personal information security and the development and utilization of personal information resources, that is, to make full use of relevant information to serve the economic and social development in the case of the protection of the rights of the information subject.

References

- [1] Su Xiaohong. Principles of Jurisprudence[M]. Law Press, 2013, p.55
- [2] Xiang Xiang. Study on Legal Issues of Personal Information Security in the Era of Big Data[D]. Beijing Jiaotong University, 2016, p.23
- [3] Lou Bin. On the Legislative Direction of Personal Information Security in the Era of Big Data[J]. Theory of Learning, 2014 (16), p.91
- [4] Zhuang Huiyan. Research on Legal Issues of Personal Information Security in Big Data Environment[J]. Journal of Yangtze University, 2015 (5), p.39