Advances in Economics, Business and Management Research, volume 110
5th International Conference on Economics, Management, Law and Education (EMLE 2019)

Personal Information Protection in the Era of Big Data

Fei Xie
China Jiliang University
Hangzhou, China

***Abstract*—From social network to online shopping, the Internet penetrates into every aspect of life. In particular, the emergence of various mobile apps in recent years has made the Internet closer to the lives of ordinary people, and humanity has entered a big data era. In this era, while enjoying the convenience brought by the Internet, the protection of personal information has been challenged like never before. How to make good use of the double-edged sword of big data, while protecting the legitimate rights and interests of citizens and creating more value for other stakeholders, will be the content of this article.**

Keywords—big data; personal information protection; problems; countermeasures

I. INTRODUCTION

The so-called big data refers to data whose size has exceeded the traditional scale, and it is difficult for general software tools to capture, store, manage, and analyze. A lot of personal information is recorded on smart apps of various computers, mobile phones, and express receipts, including names, phone numbers, home addresses, etc. Big data technology is to obtain personal information of citizens through various channels, and then use the electronic device to transfer the information and then carry out objective analysis and calculation with the help of specific algorithms to obtain some aspects of statistical information. In such a social environment where leaving the Internet seems to be derailed from the times, all aspects of clothing, food, housing and transportation, have been networked. While using convenient various online apps for shopping and planning trips, more or less personal information leaks. In such an environment, the phenomenon illegal use of various personal information is innumerable. Therefore, in the era of big data, it is imperative to define the scope of personal information and implement targeted protection through laws, strengthen the self-discipline of industry organizations, and raise the awareness of citizens' personal information protection.

II. USE OF PERSONAL INFORMATION OF CITIZENS IN THE ERA OF BIG DATA

Big data refers to a collection of data that cannot be captured, managed, and processed with conventional software within a certain time frame. It is divided into three steps: data extraction and integration, data analysis, and data interpretation. Heterogeneous data sources are extracted and integrated, and the results are stored uniformly according to certain standards. Use appropriate data analysis techniques to analyze the stored data, extract useful knowledge from it, and present the results to end users in an appropriate way. At present, big data technology is developing at an alarming rate. It will accommodate thousands of citizens in many data systems, which will not only bring about changes in government management models, but also cause changes in economic development models and citizens' daily lives.

In the process of modern management, the government collects and processes the information of each citizen to form a data system that can efficiently handle daily affairs. The effective use of citizens' personal information not only makes the two-way interaction between the government and citizens faster and smoother, but also plays a vital role in stabilizing social order and providing better public services.

While innovating government management methods, various emerging business models such as O2O services and P2P online lending that rely on network platforms are also quietly changing people's lifestyles, mainly reflected in citizens' use of personal information for website registration as access to the network Pass, the enterprise obtains effective information through the network data platform, analyzes and processes the screened valuable information, understands the needs and preferences of customers in a timely manner, and then makes the most feasible decision according to the time. In today's big data era, how to balance the impact of big data technology on personal information of citizens and how to protect the personal privacy of citizens requires further thinking.

III. PROBLEMS IN THE PROTECTION OF PERSONAL INFORMATION OF CITIZENS IN THE ERA OF BIG DATA

A. Irregular Collection of Personal Information of Citizens

Hidden information security risks are hidden behind a simple and fast lifestyle. The endless stream of scam calls and sales information, the outbreak of "naked loans" by college students, the human flesh search information posted on the Internet, and the full range of personal data required by various websites are all violating the security of citizens 'personal information. The "Xu Yuyu" telecommunications fraud case that shocked the whole country, the criminals not only stole the victim's personal information to cheat money, but even indirectly threatened the personal safety of others.

These problems arise mainly because in the daily life of citizens, there is a phenomenon of no right to collect, excessive collection, and illegal collection. In addition to some government departments and businesses, there are also unauthorized enterprises and individuals conducting illegal collection of citizens 'personal information, and even bold private investigation agencies, privately set up investigation companies to publicly sell citizens' personal information. For example, a private detective collects a series of information related to the identity, life and even the schedule of the respondent for the employer, so as to obtain corresponding compensation. This type of investigative agency takes advantage of the lack of legal systems related to the personal information of citizens, illegally collects information, and seriously violates citizens' privacy rights of personal information.

B. Citizens' Lack of Awareness of Protecting Personal Information

Citizens' personal information is arbitrarily distributed on the Internet, telemarketing continues, and even incidents of impersonation by others who know the private information continue to occur. From the root cause analysis, the occurrence of this series of events is directly related to the insufficient awareness of citizens to protect personal information. Citizens' weak awareness of protecting personal information has created conditions for criminals to take, leak, and provide information. For example, if you click on a website at any time, you need to fill in various personal information, some of which are as detailed as your home address and ID number, etc. Citizens do not realize that this is actually infringing their own information security. Some illegal websites use citizens' lack of awareness of protecting personal information, openly leaking and selling the privacy of others, causing huge hidden dangers to information security. Secondly, filling in leaflets and materials related to individuals at random every day increases the possibility of information being used illegally. In recent years, there have even been incidents of falsifying other people's information in place of others. This has seriously exceeded the scope of information security and has risen to the level of disrupting social order.

C. Poor Supervision by Government Departments

When the government protects the personal information of citizens, the regulatory boundary is often blurred. This is mainly due to the unclear concepts, lack of rules and regulations in the management process, and the absence of an independent information supervision department for special management, which leads to unclear responsibilities and low work efficiency of each department. At the same time, the era of big data relies on the network as the background. There are many Internet users, diverse information and diverse data, and it is difficult for government departments to manage it in detail. And because of the lack of a set of norms and regulations for network information management, it is easy for the government to lack regulatory enthusiasm and neglect citizens' personal information management. In addition, a small number of government workers are driven by their interests to obtain and illegally sell other people's information without permission to use their positions, causing adverse effects on society.

IV. Reasons for Insufficient Protection of Citizens' Personal Information in the Era of Big Data

A. Market Interest Driven

The development of the commodity economy and the market economy has made data the equivalent of money in the information age. Whoever can process the obtained information more efficiently can get more market resources, and who can screen out the most valuable information can have a cutting-edge perspective. As a result, personal information of citizens has become a saleable item in the eyes of criminals. To this end, they take risks at the expense of others to gain their own interests. For example, in the "Xu Yuyu" case, scammer Chen Wenhui and others purchased personal information of candidates through hackers online, and successfully cheated Xu Yuyu Gang's registration fee of nearly 10,000 yuan in just 4 hours. Throughout the entire fraud process, hackers who obtained other people's information through illegal channels and resold to criminals to defraud other people's property have seriously violated the law.

In China, public institutions collect the most information. In addition, the real estate agency, sales, and logistics industries, which are in close contact with citizens' personal information, also hold a large amount of data. In the information age, driven by their interests, these people in the industry at the risk of being sanctioned by the law, leaked and sold information about others.

B. Lack of Citizens' Personal Information Protection Education

Although action to protect citizens 'personal information is imminent, citizens' awareness of self-protection remains weak. This is mainly because the government has not yet formed a systematic theoretical system, and the lack of education and awareness of citizens 'information security consciousness, coupled with the fact that the protection of citizens' information security has not been incorporated into the government's work priorities within the department, has not formed a complete set of theoretical logic for citizens. Concept is vague and lacks awareness of protecting one's rights. On the one hand, it does not form a strong legal concept and lacks self-discipline. It is easy to take risks and obtain illegal benefits through illegal sales and disclosure of other people's information. On the other hand, due to the failure to obtain relevant legal knowledge and a good legal atmosphere of learning, knowledge and usage, citizens cannot use legal weapons to protect their legitimate rights and interests when personal information is violated.

C. Imperfect Laws and Regulations

In 2009, China's Criminal Law Amendment (VII) was promulgated. This is the first step in protecting the personal information of citizens in China's criminal law. It criminalizes the behavior of "selling, illegally providing, and illegally obtaining" citizens' personal information. In 2015,

the Criminal Law Amendment (Ⅸ) revised the provisions on personal information crimes, mainly including two aspects. One is the expansion of the scope of crime subjects, and the other is the expansion of the scope of criminal acts. Although China is gradually improving the legal deficiencies in the protection of personal information of citizens, overall, the form of decentralized legislation in our country is not perfect, and there is no complete and systematic "Citizens' Personal Information Protection Law". There are still "unreliable" situations. This has caused great distress to government departments in information management, and the ambiguity of related legal concepts has also made it impossible for civil servants to find legal basis and increase the difficulty of supervision. At the same time, the government supervision department still has the phenomenon of focusing on collection but not management. It only enjoys the convenience brought by the huge data system, but negatively handles the weak links in information protection.

V. Countermeasures for Citizens' Personal Information Protection in the Era of Big Data

A. Strengthening the Audit of Information Collection Subjects

For entities such as websites, social media, and application platforms that require users to submit personal information for registration, the government must conduct a strict review to clarify the scope of authority of the responsible party to prevent excessive collection of information during the data collection process, even if it is not authorized illegal collection of information from others occurred. During the review process, collection standards should be established to determine whether the collection subject is qualified to obtain information from others. Regarding the specific content of information collection, it is necessary to strictly address concerns at the source to prevent the occurrence of illegal information acquisition of citizens.

B. Raising Awareness of Citizens' Personal Information Protection

First of all, the government should put the protection of citizens' personal information security into its work priorities. Today is an era of "Internet +" and "Big Data". However, some government regulatory departments have not adjusted their work plans and priorities according to the circumstances. Maintaining the security of citizens' personal information plays a vital role in stabilizing social order. It is also the government's obligation to give citizens a sense of security and trust.

Secondly, regular information security education must be provided to citizens. Most of the information leakage originated from the network platform, and most citizens voluntarily filled out their personal information in the process of using the network, and leaked important personal information invisibly. The government shall carry out publicity and education activities on network information security to make citizens realize the importance of protecting personal information and prevent the possibility of information leakage from the source. Citizens are required not only to protect personal information and safeguard the legitimate rights and interests of individuals, but also to respect the personal information of others and not violate the privacy and security of others.

C. Strengthening Government Supervision

The government should strengthen the construction of industry ethics and supervision, and establish corresponding rules and regulations. For enterprises that do not use information within the prescribed scope and illegally leak and use citizen information, the government should severely punish them. Secondly, the government should lead large enterprises to take the lead, establish the concept of protecting the personal information of others, be free from the temptation of interests, abide by professional ethics, and use citizen information reasonably within the permitted range. At the same time of education, formulate uniform rules and regulations, and take punishment measures against employees who arbitrarily leak user information.

In addition, the stability of the information platform determines the security of the data. The government and other collection entities must effectively supervise and maintain the platform system to prevent the data server from being maliciously attacked by criminals and leaking personal information. Increase capital investment in big data servers, carry out regular maintenance upgrades, and timely patch system vulnerabilities to minimize the possibility of personal information leakage.

VI. Conclusion

In the context of the big data era, personal information security is becoming increasingly important. It brings a convenient lifestyle, but it is also used by criminals as a tool to obtain illegal profits. How to make good use of this double-edged sword and use big data to create more wealth for all sectors of society while preventing personal information from being leaked and used in violation of regulations requires the joint efforts of the government, enterprises and citizens, and it is also the responsibility of the government.

While strengthening its own construction, the government should actually start from the weak links in information protection, formulate industry norms and supervise the strict implementation of various industries, protect citizens' information from being infringed, thereby creating a good social environment and promoting the healthy and prosperous economic development. Although the situation of protecting the personal information security of citizens is still severe, it is believed that with the joint efforts of the government, enterprises and individual citizens, a stable, harmonious, trusting and prosperous society is ahead.

References

[1] Xiaofeng Meng, Xiang Ci. BigData Management:Concepts, Technologies and Challenges [J]. Computer Research and Development, 2013, 50 (1).

[2] Zhizhi Cao. Analysis of Information Security Issues of Chinese Citizens in the Context of Big Data [J]. Legal Expo, 2018: 10-11.

[3] Lily Yang. Criminal Law Protection of Citizens' Personal Information under the Network Environment [J]. Journal of Kaifeng Institute of Education, 2017, 37 (7): 229-230.

[4] Zipei Tu. Big Data [M]. Guilin: Guangxi Normal University Press, 2012.

[5] Aimin Qi. General Discussion on Personal Information Protection Law-Rescuing Personality in the Information Society [M]. Beijing:Peking University Press, 2009.

[6] Jiulong Liu. Research on the Legal Protection of Personal Information in the Big Data Era [J]. Legal System and Society, 2017, 8 (below): 63-64.