ATLANTIS PRESS
Advances in Economics, Business and Management Research, volume 94
4th International Conference on Economy, Judicature, Administration and Humanitarian Projects (JAHP 2019)

Privacy Protection of Personal Information in the Context of Big Data

Xiaoyu Luo
China Jiliang University
Hangzhou, China

***Abstract*—Nowadays, China has entered the era of big data, and people's lives, work and learning are all affected by the big data of network platform. In the era of big data, privacy protection of personal information should be paid more attention to. Starting with the concepts and characteristics of big data and personal data, this paper will analyze the potential security problems brought by big data, and then put forward some opinions and suggestions on the privacy protection of personal information.**

***Keywords*—big data; privacy protection; data security; personal information**

I. Introduction

With the development of the computer and Internet industry, the status of information in modern society has gradually increased, and so has the reliance on information in all walks of life. As an important resource, information can bring infinite value after being collected and analyzed and the big data age is born in this situation. Through the collection and analysis of personal information of network users through the latest computer technology, the value beyond the information itself is mined. The wide application of big data in various industries has also brought certain hidden dangers to personal information security. Massive data always records people's lives. Data mining technology brings people more precise and personalized services, whereas personal information is exposed to the air. Therefore, in the era of big data, the greater the development of data is, the greater the risk of personal information will be "sneaked", and the more serious the leakage of information will be. The issue of information security protection should also attract the attention of the public, enterprises and even the country.

II. Privacy of Personal Information

A. Concepts and Characteristics of Personal Information

Personal information refers to information that is relevant to an individual and that can be used to directly or indirectly identify a particular natural person. National and regional personal information protection regulations have already given legislative provisions on the definition of personal information. As stated in the OECD's Guide to Privacy Protection and Cross-Border Movement of Personal Data, "personal data refers to any information about a natural person that is identified or can be identified"; in the UK's Data Protection Act, "personal data refers to data that is identifiable and relevant to the surviving individual; based on which the individual can be identified, or based on such data, the data controller may obtain additional information to identify the individual". [1] In addition, there are France's "Data Processing, Data Files and Personal Freedom Act", the European Union's "Personal Data Processing Protection and Free Flow Directive", Germany's "Federal Data Protection Act" and so on. What these regulations have in common with the definition of personal information lies in that the core of personal information is the identification standard. In addition, personal information also has the following three legal characteristics: identifiability, personality attributes and property attributes, and objectivity. [2]

Firstly, it is the identifiability of personal information. The identifiability of personal information includes direct identifiability and indirect identifiability. Direct identifiability means that a person's identity can be directly confirmed through a single message, including personal identification number, gene, name, etc. Indirect identification means that a person’s identity cannot be directly confirmed through a single message, but it can be confirmed by combining other information or compared with other information, including address, gender, occupation, and contact information. Therefore, the identifiability represents one important criterion for judging whether some information constitutes personal information, and only when there is an identifiable objective connection between specific information and specific individual can personal information be constituted.

Secondly, it is personality attributes and property attributes. On the one hand, personal information carries personal interests, such as improper disclosure of personal information, improper alteration or distortion of personal information, illegal commercial use of personal information, and the use of personal portrait information, etc. They are all manifestations of violations of personal interests. On the other hand, the value of personal information includes both spiritual and economic values. Although property and personality are obviously different, property has economic value and can be separated from the subject, but the boundary between property and personality is not absolutely clear. Some property rights have personal characteristics that are inseparable from the subject, such as the claim for maintenance. Under certain conditions, some elements of personality can be separated from the subject and possess property, such as name, portrait and privacy.

Finally, it is the objectivity of personal information. Personal information is a record of a person's physiological characteristics or social activities. It is a reflection of the true existence of an individual's situation. It is an objective existence, not a subjective creation. This is the objectivity of personal information. Personal information can objectively and accurately reflect an individual's personality behavior or habits, etc., so that it is of great value. Conversely, the data information that is separated from the specific person, things, and things recorded is meaningless and worthless.

B. The Relationship Between Personal Information and Privacy

The traditional privacy right in China refers to the personal right of private people to own the privacy of private life and information secrets, and is not subject to illegal intrusion, knowledge, collection, use and disclosure by others. Although Chinese laws do not have a clear legal provision on privacy, there are many legal provisions in China that are related to privacy rights, such as the constitution's protection of citizens' personality, housing, communication freedom and communication secrets; criminal law on citizens' bodies, housing, reputation, freedom of communication, and protection of personal information; civil law's protection of citizens' portrait, reputation, name, and name rights; in addition, Chinese Tort Liability Law also has a more detailed provision on the scope of citizens' privacy.

From the definition of personal information and traditional privacy rights, the value tendency of personal information is different from that of traditional privacy protection. The value of traditional privacy protection tends to be human dignity, while the value of personal information protection tends to personal dignity and the free flow of data. At the same time, the field of privacy protection and the field of personal information protection are both inclusive and intersecting. Privacy not only protects personal information but also personal space. Some American scholars divide the interests of privacy protection into four categories: information privacy — personal control of the interests of others in controlling their own information; domain interests — controlling the interests of intrusive behavior; body privacy — controlling the body to avoid the benefits of interference; communication privacy — controlling communication from the interests of surveillance and confidentiality. Thus, personal information protection is included in the protection of privacy. The relationship between privacy protection and personal information protection is as follows: first, personal information is reflected in the internal and external characteristics of the person; second, privacy includes some private personal information, including non-personal information content such as private life and residential tranquility and privacy is not public; finally, the parts of personal information do not constitute private content when they appear alone, and some personal information combinations may become private content when they appear. Second, privacy includes some private and non-personal personal information such as private life and residential tranquility that is not public; finally, some parts of personal information do not constitute private content when it appears alone until they appear as a combination.

It can be seen from the above, in the era of big data, only the legislative protection of privacy rights is very thin, and it is difficult to bear the legal responsibility of the complicated and diverse personal information leakage and trading in the network society. Therefore, establishing a personal information protection mechanism is an urgent task.

III. Information Security in the Context of Big Data

A. The Concept and Characteristics of Big Data

Big data is a collection of data that cannot be captured, managed, and processed by conventional software tools for a certain period of time. It is a lot of decision-making, insight, and process optimization capabilities that require new processing models, high growth rates and diverse information assets. Big data is characterized by 4V+C, namely, Volume, Velocity, Variety, Value, and Complexity. Big data is bulky, structurally diverse, and time-sensitive. New technologies such as new computing architectures and intelligent algorithms are needed to process big data. [3] The application of big data emphasizes new ideas to assist decision-making, discover new knowledge, and emphasize online closed-loop business process optimization. Therefore, big data is not only "big" but also "new", which is a combination of new resources, new tools and new applications.

The development of the Internet industry in recent years has led to the application of big data to all walks of life and has shown a step-by-step development. From Internet technology to business, finance, medical care, education, etc. big data is being actively tried, and the massive data collected by big data has also enabled all industries to tap into value. Even governments and other related agencies have begun to use big data as tools to maintain national security and citizen safety. The latest data shows that the number of Internet users in China has exceeded 800 million, of which 3.6% of netizens under the age of 10 are over 28 million. In fact, the number of real young netizens is definitely far above this number. So many young netizens will definitely be affected by some bad information on the Internet. That bad information will hurt the health of young people. Under such circumstances, government and related departments and institutions must maintain and screen the network environment and network information. At the same time, it must also monitor the network usage of individual users on the Internet to prevent people from using the network to disseminate bad information and Video, etc. Under this means of prevention and monitoring, China can create a safe network environment, and a safe network environment is conducive to the healthy development of young people's physical and mental health. However, big data has brought great convenience to modern society, and it has also brought about the security risks of personal information and privacy.

B. Security Hidden Dangers Caused by Big Data

With the development of Internet technology, the collection and analysis of big data is becoming more and more accurate and the field of big data applications is expanding and the protection of personal information security has become tense.

Each of us is the producer of information. In the big data living environment today, everyone's every move, words and deeds will be collected and recorded by big data. In real life, mobile phone has become a tool that can't be separated from people's convenient life. By downloading and using the apps in the mobile app store, it is easy to order takeout, shop and take a taxi. These apps make modern people enjoy the convenience and speed of online life. But before using it, the app will let users agree to a privacy policy and allow the app to read the text messages, contacts, geographical position, photos and even calls or social chats on their phones during the process. If someone doesn't agree with these, he or she will not be able to use the app. This is a common way of collecting personal information in daily life.

But in is not as long as people's personal information is collected that it is valuable. The real value of personal information is realized through the sale of information and the analysis of information. The sale of personal information, such as the platform to sell the user's mobile phone number to another platform or other institutions, or even fraudulent gangs, the platform has obtained a certain amount of income by selling user information, and this income is still quite a lot, because of its vast land and large population, China can be said to be an “ocean” of information, it will have great value. Subsequently, the user is arbitrarily harassed or scammed because he or she has been sold to other platforms or agencies or fraudulent gangs. Moreover, the collection and analysis of user information by a platform finds the user's personal privacy, such as some problems with good or sexual orientation. In fact, this "harassment" and "peek" have seriously affected the normal life of modern people. It goes without saying that everyone does not want to live in a state without a "protective layer." It's like human beings without clothes. But in fact some of personal secrets are also hidden, so in this densely populated society, there is a sense of security.

But in the context of privacy, the concept of "harm" is much more difficult to define. [4] Since personal information can also be included in the privacy right, the concept of "harm" in the context of personal information security protection is also difficult to define. Because it is often difficult to prove that life is exposed to information, which is hurting people. For example, being eavesdropped on the phone usually does not lead to a material loss. Just as someone is stolen, it difficult to show what his losses are from the angle of personal information: collection and analysis. It seems that the "security" people seek is only a psychological comfort, and there is no substantial thing that allows to prove this security. In addition, it is still to be considered whether the use of big data "killing" for price discrimination on the Internet platform has caused a legitimate right to the user. Moreover, many people are unconscious about the security of their personal information, so it is necessary to publicize and educate the online users about their awareness of privacy protection.

For the Facebook user information disclosure incident that has caused widespread concern, the personal information of 87 million users has been acquired and analyzed by political companies, and even has a certain influence on the US election. This shows that in the era of big data, inadequate personal information protection not only brings personal security risks, but also has a great impact on economic trade and politics.

IV. Suggestions on Personal Information Security Protection

Therefore, this paper puts forward the following suggestions for the security risks of personal information in the above-mentioned large data environment:

A. Strengthening the Awareness of Personal Information Security Protection of Network Users

Since many online users do not know that big data will be analyzed after collecting personal information, and use it to obtain the corresponding value, it is necessary to publicize and educate the network users on the protection of personal information security protection. Let every network user know that you can't fill in personal identification information, personal network account information, bank card number, etc. on the network.

B. Increasing Research and Development Efforts on User's Personal Information Security Technology Support

Mobile terminals are now a very common web tool, and people can use their mobile phones to shop, socialize, and so on. So a mobile phone stores a lot of personal information about users, such as phone number, identity information, home address and even work units, so efforts should be strengthened in the protection of mobile terminal personal information. There are already some protection methods, such as fingerprint unlocking and portrait unlocking. But the means of cracking criminals are also growing. Therefore, the technology for the security protection of users' personal information must be continuously improved to protect personal information and privacy on mobile phones better.

C. Improving the Legislation Related to Personal Information Security Protection

At present, Chinese legislation on the protection of personal information security in big data is still not clear. There is a lack of relevant laws and regulations to divide the responsibility for revealing personal information and privacy. Therefore, China should formulate relatively comprehensive and comprehensive big data legislation as soon as possible so that big data security and personal information security can be legally protected.

D. *Strengthening the Supervision of Network Platform*

The network platform should strengthen the protection of users' personal information and privacy, and the relevant agencies such as the government should also strengthen the supervision of the network platform to prevent the occurrence of incidents in which the network platform leaks user privacy. This dual supervision can more effectively protect the personal information and privacy of users.

E. *Strictly Cracking Down on Illegal Infringement of Personal Information Security*

Personal information is leaked by lawless elements, causing loss of property and even personal belongings of network users. Relevant institutions must crack down on criminals who violate the security of personal information. Due to the development of the online society, personal information disclosure cases are now very common. Therefore, it is very important to increase the intensity of crackdowns and severely punish criminals who disclose personal information.

V. CONCLUSION

The rapid development of the network makes us pay more attention to the protection of personal information security of big data. The protection of personal information needs the cooperation of the whole society from many aspects in order to minimize the occurrence of personal information leakage. Protecting the security of personal information can also promote the sound and rapid development of Chinese online society, enabling us to enjoy much more convenient network services.

REFERENCES

[1] Fan Wei. "Path Reconstruction of Personal Information Protection in the Big Data Era," the"Global Legal Review" in the 5th issue of 2016, p92-115.

[2] Wang Rong. "Data Protection and Flow Rules in Big Data Era", People's Posts and Telecommunications Publishing House, 2017.

[3] Shi Weimin: "Realistic dilemma and path choice of personal information protection in the era of big data", the "Intelligence Journal" in the 12th issue of 2013, p155-159+154.

[4] Bart van der Sloot. "Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR’s Case Law on Privacy Violations Arising from Surveillance Activities", the "Issues in Privacy and Data Protection" 2016, p411-436.