Advances in Social Science, Education and Humanities Research (ASSEHR), volume 252
3rd International Conference on Judicial, Administrative and Humanitarian Problems
of State Structures and Economic Subjects (JAHP 2018)

Research on the Legal Protection of Personal Information in China in the Environment of Big Data

Xiaoxun Huang
School of Public Administration
University of Electronic Science and Technology of China
Chengdu, China 611731

***Abstract*—With the rapid development of the Internet, the combination of virtual network and real life is becoming closer and closer, the use of big data technology makes the value of personal information more and more prominent. It also makes personal information at risk of being leaked and misused. The protection of personal information is to make better use of personal information. From the point of view of balancing the protection and openness of personal information, it is the focus of the research to design a set of reasonable personal information utilization and protection system. This subject begins with the particularity of personal information in the big data era, expounds the personality attribute and property attribute of personal information, and probes into the basis of the development and utilization of personal information. Secondly, this paper studies the unsafe situation encountered in the current open use of personal information, analyzes the causes of the current unsafe consequences, and finally puts forward some suggestions on how to perfect the ways to protect personal information security in China.**

Keywords—big data technology; personal information; privacy security; protection path

I. INTRODUCTION

The use of big data technology not only brings convenience to human life, but also makes personal information into a state of insecurity. In order to balance the opening and protection of personal information, constructing a reasonable personal information protection system is not only the basis of the healthy development of information economy, but also a problem to be solved under the environment of big data.

II. THE CONCEPT AND LEGAL ATTRIBUTE OF PERSONAL INFORMATION IN BIG DATA ENVIRONMENT

A. The Concept of Personal Information Under Big Data

From the physical technical level, information is the object that is transmitted by the signal (sound, image, text) as carrier and can be received and processed by the signal system. Whether there is a receiver or not, the physical information always exists in the objective world. From the social level, information is the content carried by the members of a society to communicate or transmit ideas. With the diversity of human social communication, the content of information transmission is becoming more and more extensive. It can be said that the extensive information content is directly related to the diversification of the means of information communication. With the emergence and popularization of the Internet, the signals of words, images and sounds can be converted into digital signals, and spread quickly with the Internet, this has greatly promoted the enrichment of information content and expression, and has led to the explosion of information in today's society.

In the physical space, once the information creators begin to disseminate the information they create, they can no longer carry out entity control over the information they create, nor can they prevent others from spreading the information they create. In big data, artificial intelligence, the Internet is still far away from human society, the way of obtaining and disseminate personal information of each member of society is extremely limited. People pay more attention to the protection of privacy right. However, after entering the 21st century, every member of the society can search for traces with the help of the Internet in the face of the developed Internet, and find the personal information directly or indirectly related to the members of the society. Once this decentralized, fragmented information has been screened, sorted out, in particular, the information database based on massive data information, it will bring huge potential benefits to the owner of the information. Literally, personal information is personal information about natural persons. According to the category of personal information protected by law, the theorists have a slightly different definition of personal information. According to the definition of "personal information" in the theoretical circle, some scholars divide personal information into three types: "relevance", "privacy" and "recognition".. "Associative type" refers to all information related to personal information, and "privacy type" refers to information involving only personal privacy, "identifiable type" refers to all information that constitutes the identification of an individual. [1] The general principles of Chinese civil law include personal information within the framework of civil law protection, but there is no clear definition of personal information. The category of personal information protected by civil law is uncertain. And scholars based on their own understanding of the definition of personal information categories are also different. In order to apply the law better, the scope of personal information protected by law must be determined first. From the point of view of the purpose of legislation and the

moderation of the category of protection, the category of personal information protected by law should not be too narrow or too broad.

B. *The Legal Attribute of Personal Information Under Big Data*

From the legal attribute, the personal information has the personality attribute and the property attribute. But under the background of big data, the property attribute of personal information becomes more and more obvious.

1) Personality: It is generally believed that the concept of personality right is linked with the concept of natural right, and it is the fundamental right of human beings. However, under the premise of illegality theory, the concept of personality right has been denied in Japan and replaced by various personality interests. [2] it can be seen that personality interests are not directly prescribed by law, and they are constantly adjusted with the development of society. Under the Internet, the diversification of personal information leads to the related personality interests. In 2010, Taiwan, China, based on the rapidly changing social environment, to strengthen the protection of personal privacy, the revision and publication of the personal data Act, expanded the object of information protection and strengthens the protection of highly private personal data (including medical, genetic, sexual, health screening, etc.). [3] In the early days of the Internet, Violations of personal information are more direct violations of sensitive personal information, such as the direct dissemination of pictures and information about individuals' privacy by means of network technology, or the use of virtual networks for human flesh searches. The verbal violence against the parties involved in some events even extends to real life, which directly affects personal life and so on. However, with the development of the Internet, especially the development of e-commerce, personal information extends to more hidden information such as personal preferences, consumption habits and so on, and the information are not completely related to personality.

The personality right in civil law is a private right enjoyed by an individual. It is naturally closely related to an individual, such as name, body, health and privacy, all of which are the basis on which an individual cannot give up and communicate with others on an equal footing. The personality of personal information is mainly embodied in the information content with privacy as the core. The right to privacy, which is based on human shame, contains two meanings: the freedom of private life to be private and the freedom of private affairs to be undisturbed. [4] In a closed and limited social environment, Personal information, especially information disclosure about privacy, may be limited to a smaller category, and individuals can avoid the influence of others on their own evaluation by means of transferring material residence and so on. But in the virtual society, personal information leakage is difficult to limit to a small scope. Because the virtual society is borderless, once it is revealed, it will be understood by all members of the society. At the same time, the concrete people in the virtual society are transformed into virtual symbols, but with the help of personal information, these virtual symbols can be directly connected with the real subjects. The leakage and dissemination of personal information will have a direct impact on the life of the real subject. The speed of information flow and the scope of dissemination are not regional, which makes the current privacy protection mechanism difficult to meet the actual needs of the public for information security.

2) Property nature: In the era of information society, especially in the boom period of electronic commerce, the scope of personal information is no longer limited to private information, but also contains some common personal information, such as personal preferences, deposits, investment methods, private telephone and so on. This general information is personal but not directly related to personality. Before the era of information digitization, the ways of retrieving and sorting personal information are limited, and the effective means of screening and combing mass information are also lacking. These non-private information related to people do not seem to be of great economic value to business practitioners. However, in the era of Internet boom, mass personal data can be effectively collated and analyzed by means of big data technology, which can not only grasp the basic situation of the individual information, but also predict the potential behavior of the individual information, and the personal information can be targeted to impose business behavior, to obtain potential benefits. When the application of personal information is used in the fields of business and economic activities, political and public policies, the accurate analysis of a large amount of personal information will have a direct impact on the economic, political and other fields. The holder of a huge amount of personal information will have a potential material benefit. Posner and other scholars believe that legal property must meet three conditions: first, scarcity and value; second, it can be owned by a specific subject; third, it can be transferred to others at a certain price.[5]

Based on the different acquisition methods, the content of personal information collection is different. The more personal information is held and the more detailed personal information is, the higher the scarcity is, the greater the value. Especially in the commercial society, when the bearer of personal credit, preferences and other personal information can often convey to the business body personal credibility and potential purchase potential, accurate positioning of target customers will reduce the cost of time and economy that may be consumed on non-target customers, improve transaction efficiency and save transaction costs. Personal information is independent of the individual, it does not depend on the consciousness of the individual subject, and it is presented through various forms, some of which are not even discovered by the individual. The holder of personal information has the right of material possession of the information he holds before the disclosure of the information he holds, but once the personal information is out of his possession, the holder of the information cannot in fact prevent others from using the information. From this point of view, those who possess personal information and take confidentiality measures have in fact taken possession of

personal information. Personal information is valuable because it is scarce, and it is transferable, of course it can be delivered at a price. From these points of view, under the information society, personal information is inherently property.

With the digitization of personal information and the diversification of data processing modes, the range of personal information has exceeded the scope of privacy in the late 19th century. There is a cross relationship between personal information based on big data and traditional privacy content. The origin of privacy is mainly passive protection, that is, it gives privacy person the right to prevent others from violating their privacy, and increases the cost of infringement by investigating the responsibility of the infringer to curb the infringer's behavior. The disclosure of privacy to the privacy of the harm is more spiritual, economic compensation may be certain compensation to the infringed, but cannot compensate for the spiritual damage suffered by the privacy. However, the leakage of personal information, such as personal savings, investment methods, private telephone, etc., obviously will not bring direct mental damage to the personal information, but once leaked, it may bring direct economic harm to the personal information. In the information society, the access to personal information is becoming more and more diversified, and the appearance is different, although the reasonable access and use of personal information will not cause undue impact on individuals, nor will it harm the public interest of the society. However, the use of big data technology may increase the possibility of improper access to and use of personal information, and directly impact on personal privacy and security.

C. Challenges to Personal Information Security in Big Data Environment

The use of big data technology to personal information has certainly promoted the progress of society. However, in recent years, the Internet burst of personal information insecurity has occurred from time to time. The use of software viruses to invade personal computers, steal personal information and control personal computers is a frequent occurrence. A global cyber attack broke out in June 2017. The uncomplicated extortion software has hacked into tens of thousands of network systems in 64 countries, requiring the victims to pay a certain fee to unlock the files. Some victims have to accept exorbitant extortion fees because they have important information on their computers or are eager to use them. But the real intent of the extortion software operator is to destroy the target system, leaving some victims unable to prevent their computer systems from being destroyed after paying for extortion. In 2016, the public security authorities detected more than 1800 cases of infringing personal information, and more than 30 billion items of personal information were seized. The number of tampered websites in China is 16758. Of these, 467 government websites were tampered with, 48.0% less than 898 in 2015.In 2016, 82072 websites were planted in the back door, of which 2361 were government websites, accounting for 2.9% of the websites that were planted in the backdoor. [6] Cambridge Analytics Company of the United Kingdom uses the 87 million user data obtained from the Facebook open interface to analyze the behavior patterns, personality characteristics, values orientation, and growth experience of the users, targeted push messages and campaign ads helped Trump win the presidential race, sparking public fears about the security of personal information and the involvement of Congress. [7]

In China, in addition to software viruses may cause computer insecurity accidents, personal information is leaked, resulting in the theft of personal funds or financial fraud by criminals are also often reported in the news. In 2015 alone, netizens lost about 80.5 billion yuan as a result of personal information leaks, spam and information fraud with an average cost of about 124 yuan per person[8]. In 2016, the figure was even as high as 91.5 billion yuan (The number of netizens in our country is 688 million ╳the average economic loss of netizens is 133 yuan = 91.5 billion yuan). Of these, 9 percent of Internet users lost more than 1000 yuan in economic losses due to various rights and interests infringements. [8] The personal information of a certain person may be only a drop in the ocean when it comes to numerous information data. However, this information is the only and most important information for those who have personal information. "The investigation report on the Protection of the Rights and interests of Chinese netizens (2016)" shows that 72% of the netizens think that the disclosure of identity information in their personal information is the most serious, these identity information includes the names of netizens, mobile phone number, email, educational course, address, ID number and other information .54% of netizens think that, including phone records and content, online purchase records, website browsing traces, IP address, Location information and other content of the personal online activities information leakage is extremely serious. The Supreme Court's case of typical crimes against citizens' personal information shows a sharp rise in the number of such crimes that began in 2015. Illegal acquisition and reselling of personal information (including household registration information, mobile phone location, accommodation records, credit information, online purchase orders, etc.) is the main means of crime. In fact, the more a person's personal information is held by others, the greater his or her personal transparency is, and the higher the likelihood of being defrauded by precision. Such incidents as Xu Yuyu in Shandong Province have long occurred in China, but in this case of precision fraud, Xu Yuyu was defrauded of 9900 yuan of tuition fees and died as a result of which more people paid more attention to the case. But this case also directly reflects that when all information is stored on the Internet, personal information security measures are extremely important. If this problem cannot be solved, the use of personal information data will be directly affected in the future.

The neutrality of technology makes technology has two sides naturally, and combines with positive purpose to produce positive effect, and combine with negative purpose to produce negative effect. Big data technology and artificial intelligence as a new technology development direction, also has two sides. But the use of such technologies should not be denied because of their potential risk of insecurity. The development of big data technology and artificial intelligence cannot be separated from the collection and processing of massive information. The combination of big data technology and personal

information to establish a new life model has brought great convenience to human life, improved efficiency, and promoted social progress. However, it cannot be denied that there are some risks in the new way of life brought by relying on scientific and technological means and big data technology, one of the most important things to watch out for is the potential insecurity of personal information. To prevent personal information from being stolen, it is necessary to set up protective barriers and guard against them by means of science and technology. At the same time, it also needs necessary legal means to punish the theft and improper use of personal information afterwards, and to use the deterrent force of the law to deter attempts to steal and use the information of others.. Constructing a reasonable personal information protection system is a necessary way to seek reasonable protection of personal information.

III. Construction of Personal Information Security Protection System for Big Data Environment in China

A. Establishing Uniform Norms for the Legal Protection of Personal Information

With the development of information technology, the problem of personal information being infringed is becoming more and more serious. Society for personal information protection legislation needs more and more urgent. Our country should issue 'the personal Information Protection Law" as soon as possible and make a comprehensive regulation on personal information protection by referring to the practice of the European Union.

At the present stage, there is a lack of special legislation for personal information protection, the State Council should speed up the formulation of administrative regulations for the purpose of protecting personal information and standardize the use of personal information on the Internet. In administrative laws and regulations, the meaning and scope of personal information under the Internet environment, the specific regulatory authorities and supervisory responsibilities of the government, the unified standards for the security of users' personal information, the ways and channels of relief for the victims should be clarified, specific measures of punishment for violators, etc. At the same time, three guiding principles should be adhered to in legislation :

1) Protect personal information and promote the coordination principle of rational flow of information: The value goal of information property right system is to balance the interests of information creators, owners, users and communicators through the setting of information communication links, and to realize the "Pareto optimal" effect of the total amount of social benefits. With the rapid development of big data cloud computing, the value of information is more and more prominent. The reasonable circulation of information can bring great economic benefits to the society and provide great convenience for people's production and life. Therefore, the protection of personal information should also promote the rational flow of information. It is embodied in the coordination of user rights and public interests, and the establishment of appropriate competition policy. Public interest is embodied in the free circulation of information, and personal information can be circulated under the condition of restriction, but this kind of circulation is based on the premise that it will not bring negative influence to the information itself. For example, whether government agencies or commercial subject are openly collecting and using personal information, the purpose, manner and scope of collection and use should be expressed, and no information other than necessary for the provision of services shall be collected.

2) The principle of minimum proportion of personal information: The leakage of personal information is mainly reflected in the process of collecting and using personal information. In the protection of personal information, the principle of minimum proportion of personal information should be adhered to, that is, the government and merchants should collect personal information on the premise of adequate use, do not collect personal information beyond your range of services in order to reserve more personal information as a resource. The percentage of personal information collected and used should be minimal.

3) The principle of legality: "The law of personal information protection" should establish legal means and procedures for the collection and use of personal information. There is no unified standard for the correct way to collect and use personal information before the relevant laws are regulated, and personal information is often faced with a state of unordered collection and use. In order to prevent this situation to continue, it is necessary to make specific legislation to clearly establish the legal means and procedures for the collection and use of personal information and to prevent the application of illegal means and procedures.

B. Strengthening the Implementation of Law Enforcement and Administrative Supervision Means

We should step up the crackdown on the new type of cybercrime, implement the supporting measures for the application and enforcement of the law, increase the cost of cracking down on the crime, and reduce the motive force for stealing personal information. Violators who have caused personal information disclosure and abuse should be punished according to law and try their best to recover the victims' losses. The government should strengthen the construction of the key information infrastructure, accelerate the establishment of the information technology system of independent R & D and production in China, and improve the security of the government computer network. At the same time, we should also guide the main bodies of the Internet industry to establish a unified safety management standard for the Internet industry subjects, reduce the unnecessary collection and utilization of personal information, establish a punishment mechanism, and increase the management and punishment within the industry, to promote the healthy development of the industry.

At the same time, the local government should pay attention to avoid infringing the personal information of the public when drawing up the local administrative norms to

clean up the laws and regulations that may violate personal information. Severely crack down on illegal means of obtaining information from others and buying and selling personal information, and strictly enforce the law no matter whether or not the act of precision fraud has serious consequences, and impose administrative or criminal penalties depending on the consequences, at the same time, a person who has been swindled can claim damages to the fraudster regardless of whether he has suffered any loss.

C. *Establishing the Stereoscopic Protection Mechanism of Personal Information with Legal Protection Measures as the Core*

The protection of personal electronic information, the law is only one of the means. Without more mechanisms, such as industry self-discipline, integrity mechanism and other related systems, legal protection may only play a certain role. Therefore, the protection of personal information should be based on the legal protection measures as the core of the overall protection mechanism.

First, establish an industry self-discipline organization. The government can actively guide enterprises to establish self-discipline organizations on the basis of the regulations of the self-discipline organization related to the protection of personal information, and establish the standard of personal information protection system, including the technical safety protection system and the system of system protection.

Secondly, the establishment of personal information collection and use of the integrity of the enterprise evaluation mechanism, if the enterprise has improper collection, use and leakage of personal information data occurred, not only directly imposed a huge amount of punishment, it also limits its ability to collect and use personal data.

Finally, in order to prevent enterprises from being unable to cope with the huge compensation caused by illegal collection and use of personal information, we should establish a risk insurance mechanism and establish a personal information risk insurance system. All enterprises involved in personal information collection must take out personal information risk insurance so as to ensure that they can pay the damage to the third party in time through insurance money if they divulge personal information and cause damage to the third party. On the one hand, it can increase the payer of compensation; on the other hand, it can urge insurance companies to supervise the behavior of collecting and using personal information.

D. *Construction of All-round Personal Information Security Education System*

The improvement of personal information protection consciousness is the key to prevent all kinds of personal information violations. It is necessary to promote the personal information security education in order to enhance the safety risk prevention consciousness of all netizens, so we can start with the following aspects:

First, the state encourages middle schools and colleges to add courses on personal information protection in the curriculum, inviting professionals to give lectures; second, With the use of news media and social forces, with the help of popular information tools such as micro-blog, Wechat, online live platform and other popular information tools, personal information risk accidents are warned to enhance people's awareness of information protection. Third, local governments take the lead to set up voluntary service agencies for information protection, and regularly go to the community for publicity and education.

IV. CONCLUSION

Under the environment of big data, the problem of personal information insecurity is prominent. It is urgent to establish an all-round personal information protection mechanism. Both legislation and law enforcement of personal information security in China need to be improved. At the same time, it is the key to construct the personal information security protection system of big data environment in China to establish the protection mechanism of stereoscopic personal information and to raise the awareness of personal information security risk prevention of netizens.

REFERENCES

[1] Bai Yun. “Research on Legal Protection of Personal Credit Information”, Law publishing house, 2013 edition, p. 9.

[2] [Japan] Wushilanqing. “Personal Rights Act”, Peking University Press，2009：7-8 pp.

[3] Wang Zejian. “Personal Rights Act”, Peking University Press， 2013:211pp.

[4] Jed Rubenfeld. The Right of Privacy, Harvard Law Review, 1989 ,VOL.102, No. 4, page 807

[5] [Americ] Written by Richard • A • Posner: The Analysis of the Property of the Economy (I), Translated by Jiang Zhaokang, China Encyclopedia Publishing House 2003 edition, p. 42.

[6] National Computer Network Emergency Technical Processing Coordination Center. China internet security report 2016[M]. Beijing: People’s Post and Telecommunications Publishing House，2017:30-32.

[7] Testimony given by Zuckerberg at a United States congressional hearing on 9 April 2018 (Agence France-Presse reports).

[8] An Investigation Report on the Protection of Netizens’ Rights and Interests in China (2015) .

[9] The Supreme People's Court Network，http://www.court.gov.cn/zixun-xiangqing-43952.html，Released on May 6, 2017.