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

Xianghua Deng¹ and Meiyuan Yan¹,*

¹Department of Law, Wuhan Donghu University, Wuhan, Hubei, 430212, China
*Corresponding author’s e-mail: yanmeiyuan@whut.edu.cn

Abstract. With the scale and convenience of information storage and transmission, human society has entered the era of big data. In this era, information has become the most valuable and potentially influential resource, and personal information that is closely related to citizens’ daily lives is no exception, and is used by all stakeholders. Improper collection of personal information, fraudulent use of personal information, and malicious use of personal information have disrupted the peaceful life of citizens, thereby threatening personal and property safety issues are gradually exposed. In the era of big data, personal information protection is facing new challenges of data personality shaping and modern power control. Strengthening the protection of personal information is an urgent need in the era of big data.

1. Introduction

The emergence of Web2.0 is a significant sign of the advent of the era of big data, and our ability to collect, analyze, and store data continues to improve. Big data changes our way of life, way of thinking, and even affects our definition of knowledge, becoming the focus of attention from all walks of life. It cannot be ignored that in recent years, while big data has facilitated human life, our information security is being threatened, and the legal protection of personal information has become a topic we must face.

On January 10, 2020, the National Committee of the Chinese People's Political Consultative Conference held a network meeting with the topic of "Strengthening the protection of personal information in the era of big data". The meeting emphasized the need to thoroughly implement and study the spirit of General Secretary Xi Jinping's important instructions on network security and personal information protection. The Party Central Committee attaches great importance to the protection of personal information in the era of big data, but our country’s existing legislation still has problems such as backward personal information protection rules and methods. Therefore, it is necessary to address the current status of personal information and strengthen the protection of personal information in the era of big data.

2. The current situation of personal information security in the era of big data

2.1. The personal information leakage is serious

With the advent of the era of big data, consumer personal information is becoming more and more important to business operators. It has become a new profit target for criminals. Random cases of reselling and divulging personal information have occurred from time to time, and the leakage of citizens’ personal information has become more and more serious. The Internet has brought convenience to our lives and made it easier for us to collect information, but it is also often used by criminals, bringing huge losses to the lives and work of citizens. As shown in the Figure 1 of the leakage of personal information,
Websites, including e-commerce platforms, search engines, portals, etc., is considered to be the most likely to leak personal information, which accounts for 14%; followed by Apps on personal information terminals such as mobile phones, PAD, smart watches, and sports bracelets, which accounts for 13%; the third is the automotive industry, such as 4S shops and telecommunication service providers, both reaching 12%; the fourth is communication software such as e-mail, WeChat, QQ, etc. And the real estate industry, including the real estate industry and communication software, reaching 11%; the fifth is express companies, accounting for 9%; the sixth is the banking and insurance industry, with 8%; the seventh is the medical, education, electricity, water, gas, etc. The public service industry takes up about 5%; the other industries are considered to be 3%, and the least is airlines and administrative agencies including air ticket agents and train ticket agents, each about 1%.

Figure 1. Personal information leakage channels

In the era of big data, citizens' information can be stolen through technologies such as big data screening and mining. As a result, the legal protection of personal information in the context of big data has become extremely difficult.

2.2. Excessive collection and abuse of personal information

In the context of online big data, accurate and detailed understanding of user preferences and needs has become a new profit method for merchants. In order to carry out accurate marketing, some merchants will use users to register accounts or purchase products to excessively collect their personal information. After that, the information was collected and analyzed, and the products that suit their preferences were continuously pushed to users, and targeted services were provided, which greatly increased revenue. However, after merchants have collected the user’s personal information, they cannot properly keep it, and even share and sell personal information without the user’s permission. In order to exempt users from publicizing user information, many apps are registered. When the user chooses the privacy statement, the user does not choose to agree to not enjoy the network service.

2.3. The personal and property safety of citizens is threatened

In this era of high-speed circulation of information, citizens have become "transparent people" under the Internet. All personal actions are recorded by the Internet, and data has the property of unlimited replication. Once personal information is leaked, it will be irreversible. Uncontrollable consequences. Professor Wang Liming once said that cases that disturb the private life of citizens, such as secret photography, secret recording, voyeurism, sexual harassment, illegal disclosure of location information, etc., are special cases arising in the high-tech era of the Internet. These cases will affect citizens. The threat to the personal and property safety is a very serious social problem that we must face[1].
3. The status quo of legal protection of personal information in the era of big data

3.1. Lack of special legislation
In the context of the Internet age, many information associated with individuals that could not be defined as personal information in the past, after aggregated comparison and in-depth analysis, has the characteristics of personal information because the information subject can be identified, and then transformed into personal information. And with the help of big data, this conversion is simple and cheap. The increase in storage capacity makes it difficult to determine the life cycle of personal information. The significance of big data technology is the ability to deeply tap the value of personal information for secondary use, which means Personal information may be processed and used for a long period of time. When traditional protection rules are constantly broken, the operability of current laws and regulations will become worse and worse, and in many related laws and regulations, the provisions on personal information protection are just an understatement, sometimes even through academic reasoning to make sure. Therefore, in today's fast-developing world, the inefficiency of existing policies and laws is obviously out of fashion.

3.2. The punishment for leaking personal information is weak
Our country’s current laws punish companies or units for disclosing personal information mostly by fines, revocation of business licenses, detention, etc. Only when the circumstances are serious, can they be sentenced to fixed-term imprisonment. In the environment of big data, personal privacy leaks often affect the lives of victims. According to my country's existing regulations on personal information leakage, only when personal privacy, reputation or economic interests are seriously damaged, the person who leaks personal information shall bear the responsibility of apologizing, compensating for losses, and restoring reputation. In my country's criminal law, when the victim suffers irreparable harm, the heavier the criminal subject bears, the greater the punishment. Most of the actual losses caused by the leakage of personal information are irreparable losses, but the corresponding punishments are not very severe. The insufficiency of penalties for leaking personal information, the deterrence to society is naturally not as great as imagined, and to a certain extent it does not play a very effective role[2].

3.3. Inadequate self-regulation by network service providers
With the advent of the era of big data, online personal information has already possessed great value. Driven by interests, some people will illegally obtain people's personal information data through collection and theft, and then apply it beyond the scope. Over-range application is that some companies use the so-called legal form to grasp personal information, but the processing of the information after obtaining the information is not as people know, and these companies may sell the personal information they obtain. In addition, in order to obtain greater economic benefits, some network service providers will also leak personal network information, which has a huge impact on the security of personal information. Some companies will mine data and information in the network, and this behavior has violated people's rights to a certain extent. When people register, these companies will say that the acquired information will be reasonably used within a specific scope, but deep mining of personal information can easily break the agreement.

3.4. Citizens lack awareness of personal information protection
The current situation of personal information leakage is serious, and the reason is related to citizens’ weak awareness of their own personal information protection. In the protection of personal information, citizens themselves are the main body of information. If they are not careful to fill in and upload personal information and have insufficient awareness of protecting their own privacy, it is easy to expose personal information to an insecure network environment. In addition, when personal information is leaked or used illegally, many citizens choose to remain silent, which makes it more opportunities for offenders. For example, in the "2019 Personal Information Security Report", 95.02% of the respondents said they had experienced an information leak, but only about 15% took action on it.
4. Suggestions for improving the legal protection of personal information in my country in the era of big data

4.1. Improve comprehensive and three-dimensional legislation

The video game industry was first created in the United States. The control of society requires the intervention of power. Law is a measure of behavior, but also an effective way of relief. It organizes and systemizes the forms of power so that power can effectively maintain and promote civilization. The most effective way to protect personal information is through legal means. However, my country’s current personal information protection provisions are scattered among various laws, and there is a lack of specialized legislation, which makes it difficult to form a comprehensive and overall protection of personal information. The "Civil Code of the People's Republic of China" came into effect on January 1, 2021. This is another result of the comprehensive advancement of my country's rule of law. It has extraordinary historical significance in the process of the rule of law in China. In Chapter VI of Personal Rights in Title IV of the Civil Code, the privacy rights of citizens and the protection of personal information are stipulated, the concept of personal information is clarified, and it is stipulated that the handling of personal information must follow the principles of lawfulness, fairness, and necessity. The relevant legislation of the Civil Code for personal information provides a civil law basis for the relevant provisions of other departmental laws (such as administrative law and criminal law), and also provides a basic legal basis for further formulating special laws for the protection of personal information. In order to protect the personal information of citizens at various levels, a comprehensive and three-dimensional legislative model should be adopted, and the "Personal Information Protection Law" should be promulgated as soon as possible to make it compatible with the "Civil Code", "Administrative Law" and "Criminal Law" and other laws in the future legal improvement work.

4.2. Increasing the cost of illegal crimes

In the era of big data, if we want to strengthen the legal protection of citizens' personal information rights, we must increase the cost of illegal crimes. In recent years, cases of infringement of personal information rights of Chinese citizens have been repeatedly banned, and even intensified. Among them, there are many criminals who knowingly cannot do it but deliberately. The reason is that the illegal and criminal cost of infringement of citizens' personal information rights is too low, and the profits obtained from the implementation of illegal and criminal acts are high, which leads many people to take risks and intentionally infringe citizens' personal information rights. Therefore, only within the scope of civil damage compensation, a strict punitive compensation mechanism is established to increase the cost of crimes committed by criminals, in order to curb the infringement of citizens' personal information at the source. In addition, while increasing the cost of illegal crimes, judicial relief channels should also be unblocked to maintain the security of citizens' personal information in an all-round way[3].

4.3. Strengthen industry self-discipline of enterprises

Enterprises become a very important subject of personal information protection, and they bear the responsibility of legally collecting, storing and using citizen information. While the legal system has yet to be improved, they need to increase their awareness of industry self-discipline, continuously improve information technology, and standardize user data. Store, use, and share standards, establish a confidentiality system, and shall not disclose, tamper with, or illegally provide information to others, and do a good job in the protection of users' personal information. In addition, companies also need to establish risk prevention and control mechanisms to complete remedial measures in a timely manner when information and data are leaked, cooperate with relevant departments to safeguard the legitimate rights and interests of citizens and social public interests, and establish a good and safe big data environment.
4.4. Improve citizens' awareness of self-protection
In the era of big data, citizens must enhance their personal information security protection awareness and develop good online habit, not easily fill in or upload personal information. When our personal information is leaked or illegally used, we should able to take up legal measures to safeguard our legitimate rights and interests [4].

5. Conclusion
All in all, the legal protection of citizens' personal information rights in the era of big data is of great significance and is related to the stable development of social economy. However, in the era of big data, while providing convenience for people's life and work, it also makes citizens' personal information security protection face huge risks. Therefore, it is necessary to improve the relevant laws and regulations, increase the cost of illegal scope, strengthen the self-discipline of enterprises in the industry, raise the awareness of citizens' self-protection, and do their utmost to protect citizens' personal information rights through the legal level.

Acknowledgement
This article is part of the research results of 2020 Provincial Department of Education Philosophy and Social Science Research General Project, Research on the Legal Protection of Personal Information in the Big Data Era (project number: 20G073).

References
[1] Wang Xiuzhe. (2018) Reconstruction of the legal protection system for personal information in the era of big data. Legal Theory Altar., 6:115-125.
[2] Martin Hilbert. (2016) Big Data for Development: A Review of Promises and Challenges. Development Policy Review., 1:22-24.
[3] Solove D. J. (2013) Introduction: Privacy Self-Management and the Consent Dilemma. Harvard Law Review., 7: 188-193.
[4] Liu Shiyao. (2019) Legal protection of citizens' personal information rights in the era of big data. People's Forum., 6: 110-111.