Legal Regulations of Personal Information Protection in the Era of Artificial Intelligence

Jing ZHOU[1,a], Huining Zan[1,b,*]

[1]*Shool of Law, Tiangong University, Tianjin, 300387, China*

[a] *3396276349@qq.com,* [b] *zanhuining@tiangong.edu.cn*

**corresponding author*

Keywords: Artificial intelligence, Personal information, Personal information protection

Abstract: Artificial intelligence technologies such as smartphones, voice assistants, and face recognition are inseparable from our daily life. In the era of artificial intelligence, our personal information protection is faced with new challenges. According to the conceptual characteristics of personal information in the era of artificial intelligence, the current situation of personal information legislation in China is combed, and the difficulties faced by personal information protection are discussed. Finally, suggestions are made for the protection of personal information in the artificial intelligence era.

1. Introduction

The term artificial intelligence was first introduced to society in 1956. With the continuous advancement of science and technology such as computers, the Internet, and big data, artificial intelligence has developed rapidly in the recent 60 years. While we enjoy the convenience of artificial intelligence such as smart homes, search engines, and voice assistants, it is inevitable that we also worry about whether these artificial intelligence machines will leak our personal information. As we all know, the joint advancement of data, algorithms, and computing power has contributed to artificial intelligence. In order to ensure the accuracy of artificial intelligence judgments, a large amount of data is needed for it to learn and use. In other words, artificial intelligence is fed by countless personal information data. If we intend to continue to develop artificial intelligence technology, we will need to provide it with a large amount of personal information. However, artificial intelligence algorithms are not perfect, and personal information leakage is not uncommon. For example, in the event of 360 Leaks, netizen only needs to search for specific keywords on the Google website to access private records of Chinese users on the Internet; information leaks such as the identity documents number of many users on the 12306 website; and more than 202 million detailed resumes of Chinese job applicants on the MongDB database have been published... With the continuous development of artificial intelligence technology and the continuous increase in the number of users, the leaked data has increased from millions to hundreds of millions. If these data are used with ill-intentions, it will cause immeasurable consequences. Therefore, the regulation of the use of personal information in the era of artificial intelligence and the protection of personal information is one of the great challenges posed in the new era.

  DOI: 10.25236/iceesr.2021.015

2. Conceptual Characteristics of Personal Information in the Era of Artificial Intelligence

2.1 Concept of Personal Information

There is not a unified definition of personal information in China. Civil Code of the People's Republic of China, Cybersecurity Law of the People's Republic of China, Provisions on Protecting the Personal Information of Telecommunications and Internet Users, and interpretation of the Supreme People's Court and the Supreme People's Procuratorate on issues concerning the application of law in the handling of criminal cases of infringing on citizens' personal information only summarize and enumerate the concept of personal information. In summary, personal information is recorded electronically or in other ways, and can identify or combine with other information to pinpoint certain information of a specific natural person, including the natural person's name, date of birth, identity document number, biometric information, address, telephone number, e-mail, health and tracking information, etc. On the basis of the Civil Code of the People's Republic of China, the second deliberated bill of the Personal Information Protection Law solicited public opinions and broadened the scope of personal information to a certain extent. It adopts the 'recognition + association' method, excluding anonymously processed information that is unrecognized and unrecoverable from the scope of personal information.

2.2 Characteristics of Personal Information in the Era of Artificial Intelligence

2.2.1 Broader Coverage

Before the era of artificial intelligence, people's general knowledge of personal information was limited to names, identity document numbers, phone numbers, and home addresses. Nevertheless, with the widening usage of artificial intelligence in people's lives, the continuous development of information network technology, the continuous increase of personal information carriers, and the continuous expansion of collection methods, personal information is no longer limited to the above-mentioned scope. Network technologists are able to identify specific individuals through browsing records, e-mails, facial information, etc. Some anonymous personal information can still identify a specific individual under certain technical means.

2.2.2 Possesses Economic Attribute

In the era of artificial intelligence, personal information not only has personal attributes, but also contains a huge commercial value. Although personal information such as web browsing records and mobile phone numbers are scattered and not profitable, when these isolated personal information form a large data set, commercial companies can analyze user preferences and needs from the data set through artificial intelligence technology, so as to formulate their next development strategy. At the same time, it also assigns labels to each user in order to accurately locate the user, conduct personalized marketing, as well as increase transaction opportunities and success rates.

2.2.3 Sharing

The development of artificial intelligence has become a world trend. We need to develop artificial intelligence, but the development of artificial intelligence requires the supply of personal information, which intensifies the conflict between the demand of artificial intelligence for personal information and the restrictions on the use of personal information. We usually will need to register and log in when we use an application. Most software will set up some convenient login methods,

such as authorized login through WeChat or QQ. This makes it convenient for the developers of the application to obtain the personal information of the user on WeChat or QQ shared between the two applications. The government also highly shares personal information. For example, in the effort to prevent and control novel coronavirus (COVID-19), various government departments have registered and collected a large amount of personal information to share information to facilitate isolation and nucleic acid testing of specific groups of people. Although data sharing facilitates our lives to a certain extent, it also increases the risk of personal information leakage.

3. Artificial Intelligence Poses New Challenges to Personal Information Protection

3.1 Artificial Intelligence Increases the Risk of Personal Information Leakage

3.1.1 Artificial Intelligence Diversifies the Ways of Collecting Personal Information

With the wide use of artificial intelligence technology in all aspects of life, the connotation of personal information continues to expand, and the ways in which artificial intelligence obtains personal information are becoming more diversified, which greatly increases the risk of personal information leakage. For example, smartphones. As a necessity in daily life, people rely on their phones to chat, shop, navigate, and so on. However, many applications on mobile phones require users to perform identity verification, fingerprint recognition, or face recognition. Unknowingly, mobile phone users allow software developers to gather specific and accurate personal information about them. In the future, artificial intelligence technology will be more widely applied in all areas of life, such as cleaning robots, smart air conditioners, smart speakers, and so on. At the same time, the user's lifestyle, work and rest habits, and personal preferences will also be recorded in real-time, becoming a part of the big data.

3.1.2 Artificial Intelligence Expands the Collection of Personal Information

The second deliberated bill of the Personal Information Protection Law established the general rules for personal information with "informed consent" as the core. However, in current practice, there are often some applications that are activated and listen to the user's conversations without their knowledge. This is because users have to agree with the applications' privacy policies in order to use its artificial intelligence technologies. For instance, the application of artificial intelligence technology in the medical field can alleviate the shortage of medical resources, improve the efficiency of diagnosis, and reduce the rate of misdiagnosis. It will also completely preserve the patient's family health history, blood type, and personal health information during the diagnosis process. The more comprehensive the personal information collected and recorded by artificial intelligence technology, the faster the update speed.

3.1.3 Imperfect Artificial Intelligence Algorithms

Artificial intelligence technology is still in the development stage and has many shortcomings. A large-scale data might be leaked if the artificial intelligence that stores a large amount of personal information is maliciously attacked by criminals.

3.2 Artificial Intelligence Makes the Subject of Infringement of Personal Information Unclear

Artificial intelligence data is likely to be used by others in the process of collection and storage, which makes it impossible for people to determine who has violated their personal information, increasing the difficulty of personal information protection. On 22 September 2017, Shaoxing

police successfully cracked the country's first case of using artificial intelligence to infringe on citizens ' personal information. They also completely destroyed 43 criminal groups, arrested 193 suspects, successfully intercepted more than 1 billion groups of stolen citizens ' personal information, and seized more than 6 million yuan of stolen money and a large number of crime tools. The criminal suspects used the deep learning technology of the artificial intelligence machine to enable the machine to operate independently, effectively identify the image authentication codes, easily bypass the account login security policy set by the Internet companies, and provide criminal tools for network fraud and hacker attacks. The professional hacker group led by Huang illegally obtained the background user data of the website, sorted the data containing various mailboxes and passwords, and they sold them accordingly to the hacker group of a collision library software. Wu and others used the data for batch matching and sold various successfully matched accounts and passwords to online fraud groups, leading to a great number of fraud cases. These fraud groups, represented by Zheng, use the acquired accounts to execute their plan.

3.3 Lack of Personal Information Relief System

At present, the protection of personal information adopts decentralized legislation, which is regulated by various departmental laws. In the era of artificial intelligence, when personal information is infringed, it is difficult for the victim to provide a complete chain of evidence to prove the violation of the information processor or information collector in accordance with the litigation rule of "the one who advocates who provides evidence". In judicial practice, the penalties imposed to the Internet companies on leaking users' personal information are mainly administrative, and the sentencing is relatively light.

4. Suggestions on Improving the Protection of Personal Information

4.1 Improve Personal Information Protection Legislation

The Civil Code of the People's Republic of China, Criminal Procedure Law of the People's Republic of China, Consumer Rights and Interest Protection Law of the People's Republic of China, interpretation of the Supreme People's Court and the Supreme People's Procuratorate on issues concerning the application of law in the handling of criminal cases of infringing on citizens' personal information, provisions of the Supreme People's Court on issues concerning the application of law in the trial of cases involving civil disputes over infringements upon personal rights and interests by information networks, and other regulations have provisions on personal information, but they are not consistent. With the promulgation of the Personal Information Protection Law, China's personal information protection has a unified standard, forming a complete personal information protection legal system that is dominated by personal information protection law and legislated separately in various fields.

4.1.1 Clarify the Rights of Users and the Responsibilities of Personal Information Processors

The second deliberated bill of the Personal Information Protection Law still considers "informed consent" as the main rule for personal information processing, but it weakens this principle to a certain extent to stimulate the innovation of the data industry required by artificial intelligence. Compared with the personal information subjects, personal information processors have certain advantages. Therefore, it should be stipulated that the subject of personal information has the right to know, the right to decide, the right to consult and copy, the right to correct and supplement, the right to delete, and the right to interpret. Meanwhile, the responsibility of a personal information

processor should be increased and emphasized[1]. For example, a more stringent imputation principle should be applied to the personal information processor in order to reduce cases where the subject of personal information loses their lawsuit due to difficulty in producing evidence.

4.1.2 Establish a Public Interest Litigation System

In practice, personal information is often sold in the form of packaging by certain elements and abused for personal gain. It is difficult for the subject of personal information to discover that their privacy has been infringed. Even if it is discovered, personal information can not be effectively protected due to high costs and difficulties in producing evidence amongst other reasons. The unreasonable use of artificial intelligence not only violates the legitimate rights and interests of citizens, but also damages social and public interests. Hence, a public interest litigation system should be established to better protect personal information. Specific suggestions are as follows: First, clarify the subject of public interest litigation. In order to select the best prosecution subject in specific cases, the procuratorial organ should fully communicate with other subjects of public interest litigation. Next, fully carry out pre-litigation investigations and evidence collection to better safeguard the public interest. Finally, cultivate information technology professionals, discover favorable clues in a timely manner, and better respond to litigation needs.

4.2 Strengthen Self-Regulation in the Artificial Intelligence Industry

The rapid development of the artificial intelligence industry is bound to bring new problems to the protection of personal information in the course of its continuous development. The second deliberated bill of the Personal Information Protection Law has been issued for public comment, but the law is stagnant and relatively lagging while the industry norms are flexible and moderately predictable. The artificial intelligence industry can regulate or formulate industry regulations in a timely and effective manner to reduce the occurrence of personal information leakage incidents. For example, the United States' Global Electronic Commerce Framework emphasizes the leading role of private enterprises in protecting online privacy and encourages self-regulation to protect personal privacy. The EU General Data Protection Regulation also adopts the concept of industry-led and moderate government intervention.

4.3 Establish Specialized Regulatory Agencies

The use of artificial intelligence has become more and more deeply rooted in all aspects of life, showing the characteristics of extensiveness and sharing, making artificial intelligence infringe on personal information in various ways. At present, the supervision of personal information in China is mainly divided according to the legal fields involved in personal information. The basis for law enforcement is different, and mutual prevarication is not conducive to the supervision of violations of personal information.

The sixth chapter of the second deliberated bill of the Personal Information Protection Law stipulates the responsible departments for personal information protection, which is the National Network Information Department. It is responsible for coordinating personal information protection as well as related supervision and management, but there are no specific personal information supervision agencies. Therefore, it is necessary to establish specialized information regulatory agencies and a unified protection standard, granting it special authority, standardizing unified management and operating mechanism, and strengthening the special supervision and management of the protection of personal information.

4.4 Improve Citizens' Awareness of Personal Information Protection

To protect personal information, in addition to the legal compliance of personal information processors when using it, it is more important to improve citizens' awareness of personal information protection, and to fundamentally reduce the occurrence of personal information leakage incidents. With the continuous enhancement of people's education level, the awareness of personal information protection is also constantly strengthened, but the relevant authorities should still increase the publicity on the damages of personal information leakage and improve the ability of personal information risk prevention.

5. Conclusion

The emergence of artificial intelligence technology has greatly improved efficiency and brought much convenience to our life. However, this new opportunity poses new challenges to personal information protection and increases the risk of personal information leakage. This paper proposes some suggestions on improving legislation on personal information protection, strengthening self-regulation of the artificial intelligence industry, establishing a special regulatory department and raising citizens' awareness of personal information protection.

Acknowledgement

This work was supported by the research project on degree and graduate education reform of Tiangong University.

References

[1] Liu, L.L.. Research on Personal Information Protection in the Era of Artificial Intelligence. Tribune of Social Sciences, no.04, pp.172-178, 2020.