Science of Law Journal (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2024.030107
ISSN 2616-2296 Vol. 3 Num. 1

Research on the Legal Protection of User Data Privacy in the Era of Artificial Intelligence

Feixuan Li

Cheltenham Ladies' College, Cheltenham, Gloucestershire, GL50 3EP, England

Keywords: Artificial intelligence; data privacy; legal protection

Abstract: In the age of artificial intelligence, users' private data are widely collected, which increases the risk of privacy leakage, and there also exists data sharing and cross-utilization. In this background, protecting user data privacy becomes even more important, so a coordinated effort is needed to develop appropriate policies and technical means to protect user privacy. This paper analyzes the current status of legal protection of user data privacy in the era of artificial intelligence, and based on the characteristics of user privacy in AI period, puts forward some implementation suggestions to further standardize the legal construction, strengthen the legal protection of user privacy and shape a harmonious and beautiful Internet environment.

1. Introduction

In recent years, with the rapid development of artificial intelligence technology, the market size of China's AI artificial intelligence industry in 2022 exceeded 284 billion yuan (as shown in Figure 1).[1] The widespread application of artificial intelligence, to a certain extent, can help break the barriers of communication and boost international communication. However, the powerful functions of data mining, storage, analysis and transmission of AI also pose potential threats to personal data privacy protection. In the path of traditional privacy protection, individuals, as the main body of privacy, are able to control the flow of personal information as well as rationally identify and evaluate various types of data collection behaviors and their harms. Nevertheless, in the age of artificial intelligence, with the continuous advancement of science and technology and the development of big data and artificial intelligence, every behavior of an individual on the Internet will leave data traces such as digital footprints or digital shadows, leading to the issue of personal privacy protection becoming a prominent issue in the era of big data. Therefore, it is necessary to continuously improve and enhance the relevant laws and regulations to ensure that the privacy and security of user data are effectively protected.

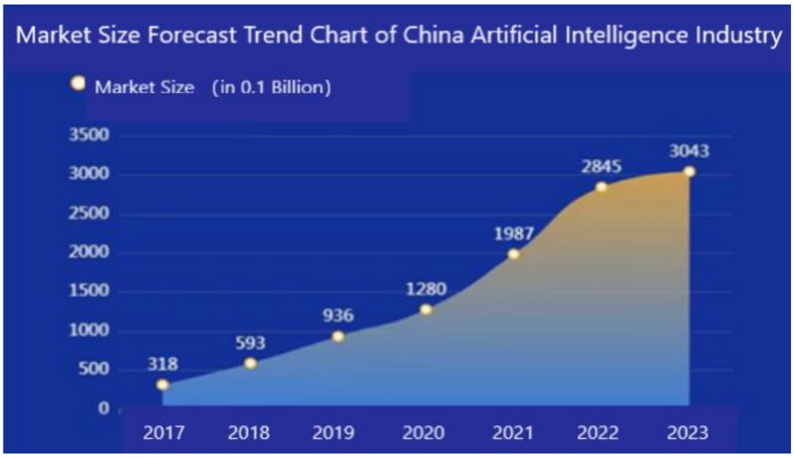

Figure 1: Market Size of Artificial Intelligence Industry

2. The Characteristics of User Data Privacy in the Age of Artificial Intelligence

2.1 Increased Risk of Privacy Leakage

In the age of artificial intelligence, a large amount of user data is being collected and utilized from a variety of information generated by individual using of the Internet, mobile devices, the Internet of Things, and other technologies, such as personally identification information, browsing history, geographic location, social media activity, etc. This information is leaked without the awareness of users through a certain process. Thus, in the age of artificial intelligence, users are at greater risk of privacy breaches due to the extensive and large-scale nature of data collection. These data may be obtained and abused by law breakers or used by organizations for commercial purposes, causing the exposure of users' personal privacy.

2.2 Challenges Existed in Data Security and Protection

In AI applications, user data from different sources may be shared and cross-used by different organizations in order to provide more accurate services. This kind of data sharing and cross-use may raise issues of user data privacy, such as data being abused or used for potentially discriminatory behavior. In addition, in AI applications, user data is often used to train machine learning models to provide personalized recommendations and suggestions to users. Although this helps to improve the user experience, it may also expose the user's privacy and personal preferences.[3]

2.3 Increased Users Awareness of Privacy

With a growing emphasis on data privacy, users’ awareness of privacy is also increasing. More and more people are becoming concerned about the collection and use of their personal data and remain vigilant about products and services that involve their personal privacy. As a result, in order to protect the privacy of user data, corresponding data security and protection measures must be taken, including the use of encryption technology to secure data during transmission and storage, as well as the establishment of strict mechanisms for access control and identity verification to prevent unauthorized access and abuse.

3. The Dilemma of Legal Protection of User Data Privacy in the Age of Artificial Intelligence

3.1 Difficulty in Guaranteeing Users' Right to Know

With the development of information technology, scope of personal information collection expands continuously. People have to allow smart devices and digital platforms to access all of their personal data, including private information, in order to better carry out social activities, handle daily affairs, and use personalized services. Even more, some IoT products can pry into people's private information and space without obtaining their "consent".[4] Study finds that users often have no idea of permission mechanisms of mobile phones. Most smartphone users are either unaware of the data collection activities of the apps on their phones or do not know what data is being collected and what its purpose is. During the testimony in the U.S. Senate, Zuckerberg acknowledged that Facebook collects information from non-social network users, which suggests that personal data may be collected when using a smartphone regardless of whether the individual uses a digital platform or not, and individuals seem to have difficulty controlling their own information and privacy. [2] However, the traditional path of privacy-empowered individuals, which defaults to the idea that privacy is only related to the individual, ignores the key to privacy protection under technological innovation. Consequently, it is difficult to guarantee the user's right to know that their privacy has been leaked when using the product, and it is hard to defend their rights.

3.2 Greater Difficulties in Individual Rights and Seeking Assistance

It is very difficult for an individual to prove the violation of privacy and to offer evidence. In traditional privacy protection, privacy is regarded as a civil right. When the privacy of a natural person's is violated, the individual is required to file a lawsuit and provide evidence to prove that the infringing subject has subjective qualification and the fact of infringement. However, in the age of artificial intelligence, it is often difficult for users to prove that a particular Internet service provider is a personal privacy data leaker, or to confirm the harm caused by the data leakage. For example, machine learning means that even if an individual refuses to use social platforms such as Facebook and Twitter, as long as others use them around, there will be a lot of data information related to them that can be accessed. Individuals cannot predict where private information will be spread and by whom it will be collected.[5] In addition, it is difficult for individuals to seek relief for collective injuries that violate privacy. Digital platforms and tech companies collect data on a large scale. By integrating and linking this individual data, they depict different groups of classification, track and summarize the group's response to different stimulation, and then advertise or conduct targeted promotions in order to obtain profits. In the process, it is difficult for individuals to seek help even when they are subjected to collective infringement such as algorithmic discrimination, big data kills, etc., because of their categorical groups.

3.3 Difficulty of Legal Supervision and Enforcement

In the age of AI, different organizations and businesses are likely to need to share user data for better service delivery or collaboration. Yet, current laws do not adequately regulate data sharing and interaction, which leads to the possibility of unauthorized data sharing and even data abuse. Moreover, due to the rapid development and wide application of AI technology, the existing legal system may not be able to follow up and supervise it in time. As a consequent, there are also difficulties in enforcing the law, resulting in the fact that violations may not be effectively penalized.

4. Suggestions for Legal Protection of User Data Privacy in the Age of AI

4.1 Establishment of Laws and Regulations for Strict User Data Protection

The government and relevant organizations need to actively enact and improve user data protection laws to clearly define the boundaries and scope of protection of individual privacy rights. These laws should keep up with the times, following up with technological developments to ensure that the law has corresponding provisions on the privacy risks of emerging technologies. Many countries and regions have adopted stricter laws and regulations to protect user data privacy. For example, the European Union has enacted the General Data Protection Regulation (GDPR), which explicitly stipulates how personal data should be collected, utilized and protected. For those enterprises which violated the regulations were imposed on penalties. Other countries are also strengthening relevant legal protection measures. [6] Therefore, in order to improve the legal system for the privacy protection, on the one hand, it is necessary to enhance the protection by restructuring the rules of infringement, etc. in the section of Personality Rights and Tort Liability of the Civil Code. On the other hand, the Personal Information Protection Law should be actively formulated to focus on responding to privacy protection issues in the age of AI.

4.2 Enterprises Actively Protecting User Information

Enterprises should establish strict personal information protection policies to ensure user data security including reinforcing the supervision of the collection, storage and processing of user data and adopting technical means to protect the security of user data. At the same time, enterprises should follow the principle of transparency in the collection and use of user data, clearly explain to users the purposes for which their data are collected and used, and definitely inform them their rights and options. Besides, enterprises should obtain the express consent from users and ensure that users voluntarily provide personal data. Finally, enterprises should take the necessary technical and organizational measures to protect the security and confidentiality of user data. For example, encrypting sensitive data, establishing strict control mechanisms for data access rights, and conducting regular scanning and repairing security vulnerability, etc.

4.3 Enhancement of Supervision and Accountability

The government should enhance the supervision of enterprises to ensure that they comply with laws and regulations related to the protection of user data privacy. For enterprises that violate the law, corresponding penalties and sanctions should be imposed to serve as a warning. First, an independent data supervisory and assessment department should be established, and a privacy commissioner is set up to form a unified and systematic supervision mechanism to provide a non-market--oriented political process for the privacy protection. Second, a corpus of privacy policies should be created to autonomously review and determine the emergence of infringements by utilizing machine learning and automated processing technology, to provide auxiliary assistance for data subjects, data collectors and data authorities, so as to generate a rational and sequential data flow order that ensures the flow of data required for economic growth while avoiding the abuse of private data. Third, personal data management systems and supervisory measures are supposed to be formulated and improved, to balance the relationship between the protection of privacy and economic growth and scientific and technological innovation. On the basis of existing data protection regulations and technologies, the risk level of private data should be further classified reasonably, the technical standards of privacy protection with the classification and grading protection standards must be unified, and the degree of infringement can be judged in combination with scenarios; the design of privacy protection for the whole life cycle should be developed, with the introduction of mechanism of the right to be forgotten to reduce and eliminate the risk and hidden dangers of privacy data leakage. Finally, international cooperation is going to be intensified in personal privacy protection. User data privacy protection is a global issue in the age of AI. Countries should intensify their cooperation in the collaborative programming unified data privacy standards and norms for the sustainable development of global data flows. The government should take the lead in construction of a data supervision and management system, formulating and improving personal data management systems and supervisory measures, playing a guiding role for public authorities.

4.4 Reinforcement of the Protection of Users' Rights

Users have the right to master and manage their own personal data. Governments should reinforce education on the protection of users' rights and raise their awareness of personal data privacy protection and establish an effective mechanism to complain and ask for assistance, so that users can conveniently safeguard their rights and interests. Breaking through the boundary restriction of "individual" as the main body in the traditional privacy theory does not mean that the individual can do nothing yet. Individuals, as relevant participants and primary beneficiaries of privacy, should still cultivate a sense of self-awareness and improve their online privacy literacy.

4.5 Innovation of Technology in User Privacy Protection

More and more privacy technologies are emerging to protect user data privacy. For example, data anonymization techniques, differential privacy techniques, etc., can protect data while maintaining the validity and availability of data, providing a better means of privacy protection for data analysis. In addition, legal protection can be enhanced through the establishment of a privacy protection agency. Some countries and regions have established specialized privacy protection agencies to oversee and enforce relevant privacy protection policies, which play a supervisory and regulatory role in promoting enterprises and organizations to comply with privacy protection norms.

5. Conclusion

In summary, as the global digitization process deepens, the further generalization and embedding of smart devices and information technology liquefies privacy into flowing aggregated data. Nevertheless, the transparent society with high-speed circulation of capital, information and communication, as well as the "black box" caused by big data mining and algorithmic technology, make it difficult for people to notice privacy leakage, or even to give up their privacy. This study analyzes the dilemma of privacy protection and the changes of real-world, aiming to provide a new theoretical perspective for understanding privacy. Taking privacy as a theoretical construction of integrated public goods, and strengthening the legal protection demonstrate the dynamic transmutation of privacy in the development of economy and society and in the process of deep global digitization. It validates the role of privacy in regulating social control and maintaining social justice and its healthy functioning, and proposes a comprehensive and coordinated path to privacy protection in order to urge governments, technology companies, individuals and other privacy-related participants to continuously adjust their policies, regulations and behaviors in the practice of economic development and technological innovation, so as to achieve privacy protection and comprehensive development of people.

References

[1] Iulian O, Anamaria V, Costin C, et al. Privacy-Preserving and Explainable AI in Industrial Applications [J]. Applied Sciences, 2022, 12(13).
[2] Calbalhin J P. Facebook user's data security and awareness: A literature review [J]. Journal of Academic Research, 2018, 3(2): 1-13.
[3] S. A C, S. J C, Ken C, et al. Synthetic Medical Images for Robust, Privacy-Preserving Training of Artificial Intelligence: Application to Retinopathy of Prematurity Diagnosis [J]. Ophthalmology Science, 2022, 2(2).
[4] Feng Yafei. Research on privacy and ethical issues of smart advertising under the technology paradigm [D]. South China University of Technology,2022.DOI:10.27151/d.cnki.ghnlu.2022.004066.
[5] Qiong Wu, Baochen Yang, Na Guo et al. Reflections on medical data protection in the era of artificial intelligence and big data[J]. Artificial Intelligence, 2022(01):54-61. DOI:10.16453/j.cnki.ISSN2096-5036.2022.01.006.
[6] Fang Xiaochuan, Hong Xieyi, Zhu Zihui et al. Privacy protection based on artificial intelligence perspective[J]. Chinese and foreign entrepreneurs, 2020(16):231-232.