Research on the Legal Protection of Personal Information Security in the Field of Artificial Intelligence

Xiaoling Zhang, Xiao Zhao

Xi'An University of Technology, Xi'an, Shaanxi, 710054, China

Keywords: Artificial intelligence, Personal information security, Legal protection

Abstract: With the popularization of artificial intelligence, personal information security in the field of artificial intelligence has also become a current hot topic. Personal information has a higher value meaning in the current development of the times, and it also supports the smooth operation of artificial intelligence systems. The current collection of personal information includes many forms, and the state presented on this basis is also different. Because artificial intelligence may collect personal information under different circumstances, it is difficult to determine whether it violates the law. This also requires current artificial intelligence. The development of the field should focus on personal information security and effective protection of laws. This article discusses the problems of personal information security in the field of artificial intelligence, considers the legal regulations of personal information security protection, and builds an effective responsibility system for personal information protection, in order to positively promote the development of artificial intelligence.

1. Introduction

At present, artificial intelligence has gradually become a hot topic, and it has gradually risen to a "competition" among countries. Countries have successively formulated artificial intelligence development projects, and my country has also actively followed the global development trend, established artificial intelligence innovation experimental areas, and gradually explored the development direction of artificial intelligence. The use of artificial intelligence can bring a series of changes to human society, and it will have a deep impact on the future development direction and the actual life of human beings. Artificial intelligence also brings certain challenges to legal content and research, and there is still a lack of relevant research on human rights and intellectual property rights. The development of artificial intelligence should not only represent advanced intelligent systems. The wind should be developed reasonably based on personal information security and legal aspects.

2. Analysis of the Problems Existing in the Collection and Processing of Personal Information by Artificial Intelligence

With the development and update of science and technology, artificial intelligence is very different from traditional information collection methods. Traditional data collection is based on paper materials, and the content is relatively different. And artificial intelligence can collect users or users' personal information through a variety of ports or web content. These ports are very common in people's daily life, including but not limited to mobile phone fingerprint recognition systems, mobile phone anti-theft positioning systems, driving recorders, etc. There is also a possibility of artificial intelligence systems in areas that we have not yet realized. When this type of smart port collects personal information, it is difficult for users to detect that their privacy has been leaked, and they lack the necessary protection attempts, and they will not track where their personal information flows and what purpose it is used for. For example, most of our mobile phones are unlocked with fingerprints and facial recognition. The user's concept only stays at the level of using the mobile phone, but does not think deeply about whether this information will be used in other ways. Artificial intelligence not only exposes personal information to the risk of leakage, but also poses a

DOI: 10.25236/edssr.2020.045

certain potential threat to the development of the country and society.

Artificial intelligence is based on people's passive application of intelligent systems, gradually expanding the scope of information collection, and the process is relatively hidden, so that users cannot detect it in a short time. Traditional information collection is mainly based on human tracking methods such as monitoring and tracking, while artificial intelligence based on big data and autonomous analysis algorithms can collect information that cannot be collected by traditional collection methods. As a current artificial intelligence product, chat bots can analyze each other’s mental activities like humans, and users will reveal their own information unconsciously, and even through algorithms, they can learn more about users’ personal information.

In addition, the autonomous learning ability of artificial intelligence is gradually improving. The future life of human beings may be flooded by various artificial intelligence services, such as cooking, chatting, etc. The intelligent system will detail the user's preferences and interests. Record and gradually achieve the purpose of collecting information. With the conversion of artificial intelligence usage rights, personal information will be disseminated multiple times through the Internet. Through the analysis of the artificial intelligence code, personal information can be seen in the eyes of professionals, and there is no corresponding privacy protection for personal information at all [1].

Artificial intelligence has a certain scope of operation for data collection, but the current purpose and scope of use have greatly exceeded the original limits, and the development of new technologies will inevitably bring more personal information protection issues. Judging from the current level of development in the field of artificial intelligence, it is not too difficult to collect personal information. However, to collect and process such users without their knowledge, it is necessary to formulate corresponding laws and regulations in a timely manner from the legal level. The boundaries and content will be used for comprehensive regulations.

3. Thoughts on the Legal Regulation of Personal Information Security Protection in the Field of Artificial Intelligence

my country still has no corresponding legislation on personal information security. Under this circumstance, it is difficult to determine whether artificial intelligence involves personal information security issues, which will have a certain impact on ethics and social morality. Compared with foreign countries, our country's legislative system is not yet mature. Some European and American countries attach great importance to personal information and actively formulate corresponding laws and regulations. my country can learn from the development experience of foreign countries and improve the network development environment to promote the corresponding improvement of the legal system [2].

Artificial intelligence is in contradiction with the protection of personal information in the process of creating its value. This requires legislators to regulate and restrict accordingly. The security of users’ personal information cannot be exchanged for the advancement of intelligence. This not only goes against the original intention of the development of artificial intelligence, but also brings certain hidden dangers to social production. Nor can it completely block the sources of personal information and hinder scientific progress. Users should have the right to choose when it comes to artificial intelligence, and not just want to protect their own information and refuse to use artificial intelligence. For example, when people use software that can be used offline, the developers of related software can strengthen the form of protection of personal information based on the demands of offline use, so that users can have the right to choose, which is conducive to the establishment of a legal system.

In addition, the law must also clarify the direction of personal information collection. Artificial intelligence builders design related programs for artificial intelligence, and do not interfere with the normal operation of the program, and do not perform unnecessary operations. It is the goal of the artificial intelligence system to complete the system independently. After the user has clarified the development direction and purpose of the artificial intelligence content, he can independently choose when to proceed with the next step, and leave the direction of personal information to be used by himself. For example, in response to the Taobao incident some time ago, some people pointed out that it used users' microphones and other devices to collect user conversations and other content, and pushed big data analysis products for them. Although relevant personnel have already explained, the boundaries of the use of some service functions are still blurred. Such disclaimers and service instructions not only fail to effectively protect users' personal information, but also cannot make effective rulings when related disputes occur. In business, artificial intelligence can effectively stimulate consumers to consume and use user data to make business profits. After personal information is clarified in laws and regulations, this development direction can be further improved based on the needs of users. my country's laws in the field of artificial intelligence still have a lot of room for improvement. The protection of personal information security is a right granted by the law and an effective way to strengthen the legal basis.

The current cybersecurity law stipulates that the collection of personal information requires the consent of the party to be collected, but this regulation still cannot effectively resolve the contradiction between artificial intelligence and personal information. When collecting user information, many smart applications omit the user's consent option or the right to know, and directly use the default form to allow users to use it without their knowledge. In data analysis and application, users' emotions and demands are often ignored. At present, the state must actively formulate relevant legal provisions to fundamentally solve this development problem. First of all, artificial intelligence developers should develop intelligent applications that meet the needs of users based on the analysis and development direction of personal information data, and use legal means to obtain personal information [3]. Secondly, artificial intelligence developers should further implement the instructions for knowing, and after obtaining the user's consent, collect relevant information reasonably to protect the user's right to know. Finally, in each step of the collection process, the user's authorization must be obtained, especially for sensitive private information, and obvious prompts or inquiries must be made. It does not involve forced users to choose options or content, and protects users' right to choose by themselves. .

4. Construction of an Effective Accountability System for Personal Information Protection in the Field of Artificial Intelligence

First of all, we must determine the responsibility system of artificial intelligence to avoid the inability to determine the subject of responsibility in the event of infringement. In the current development of artificial intelligence, an effective management system has not been formulated, especially in the division of subjects. There has been no clear boundary. Artificial intelligence, as a way to collect data, should not be its own subject, but should be based on actual conditions. The operator, as the main body, can be held accountable for infringement of personal information. The development of artificial intelligence is based on the moral standards of human beings and the laws of society [4]. Regardless of the level of development of artificial intelligence, it should not override the development and survival of human beings. It should conform to the natural development direction and laws to avoid disputes between artificial intelligence and human development, and eventually lead to artificial intelligence development beyond human expectations. It will threaten the development of human beings, and even the right to survive will be deprived.

While developing artificial intelligence, related products must also accept management and control measures to strengthen the protection of user information. First of all, in terms of product performance, a series of testing standards must be established, and testing should be carried out in time before leaving the factory and during use. Prevent its defects and lead to leakage of user information. In the process of sales and after-sales, if there are serious product defects or leaks, the problem products should be recycled in time, and the service system of the problem equipment should be stopped to effectively block the leakage of user information. In the development of artificial intelligence, it is necessary to strengthen the management and control of the field of artificial intelligence, and strengthen the ethics of relevant practitioners to form good self-discipline and management capabilities. After artificial intelligence products are put into use, relevant production organizations must invest corresponding maintenance costs or purchase insurance for them. In the event of accidents, they must provide corresponding protection mechanisms for users and production organizations.

Enterprises must also obtain a certain right to know when operating. When disputes occur, the enterprise can divide the responsible persons according to the use agreement between users and related content. When a major information leakage incident occurs, the enterprise should report to the relevant agency in a timely manner and seek the help of an authoritative agency to minimize the impact. When artificial intelligence is processing personal information, companies must clearly divide the privacy rights of users to prevent artificial intelligence from exceeding its prescribed scope in the process of collecting information [5]. For companies that violate the regulations, relevant management agencies must formulate penalties in a timely manner. my country’s relevant management content only provides for property punishment, but artificial intelligence and the value of personal information have great development value. Therefore, while managing, it is necessary to further improve the punishment rules. For bad and serious circumstances, the criminal law can also be used. Incorporate into more specific management. The current foreign penalties for infringement of personal information are mainly fines, which can even be used as the country's turnover. my country can also learn from some foreign measures to standardize the development direction of domestic artificial intelligence.

5. Conclusion

In summary, under the development of big data, the development of artificial intelligence has gradually deepened. As the core element in the field of artificial intelligence, the use of data will have a certain impact and change on the basic life of human beings. This also requires that while developing artificial intelligence, the ability of individuals to protect and identify information must also be strengthened. Technological innovation is the inevitable development of the times. Therefore, we must actively establish an effective management system and legal system to deal with the protection of personal information in the field of artificial intelligence. Enterprises should also formulate relevant standards within the company to ensure that the development of artificial intelligence integrates all aspects of development needs, and thinks from humanities, laws, and ethics to ensure that the development environment of artificial intelligence is consistent with the overall development direction of society.

References

[1] Zhu Gaofeng. On the legal protection of personal information security in the field of artificial intelligence. Journal of Chongqing University, vol. 26, no. 4, pp. 150-160, 2020.

[2] Zha Yuhan. Research on the Legal Issues of Personal Information Data Security in the Field of Artificial Intelligence. Think Tank Times, vol. 2, no. 8, pp. 250-251, 2020.

[3] Song Ping. Research on Personal Information Protection in the Application of Artificial Intelligence. Hebei University, 2019.

[4] Miao Wensheng. Legal regulations on personal information data security in the era of artificial intelligence. Guangxi Social Sciences, vol. 9, no. 2, pp. 101-106, 2018.

[5] Wu Qiong. On the protection of big data security in criminal law in the era of artificial intelligence. Journal of Hubei Normal University, vol. 38, no. 4, pp. 56-58, 2018.