Science of Law Journal (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2023.021224
ISSN 2616-2296 Vol. 2 Num. 12

Reflection and Analysis on Data Security Risks and Legal Research in the AI Era

Xingjia Lu

Law, UNSW, Sydney, 2052, Australia

Keywords: AI era; Data security risks; Legal research; Thinking; Analysis

Abstract: This article conducts a study on data security risks and laws in the era of AI. In the development of AI, the lifecycle of data, especially data security protection, is a key concern. The AI data security brain utilizes billions of intelligent terminals to collect data and information, and through intelligent analysis, perceives security risks; Possess the ability to self-learning and self-evolution to identify new threats. In order to promote data empowerment, ensure data security during the development of AI and ensure the driving role of data in the development of the digital economy. Establishing the Basic Law on Maintaining Data Security requires the establishment of basic principles of data security, the regulation of basic maintenance systems, and the formulation of core content for maintaining data security. And reduce the query security risks faced by the data to the smallest possible extent, thereby ensuring the legitimate and reliable query of the data. Data security issues have become prominent, and China has accelerated legislation to protect data security in the development of AI at the legal level.

1. Introduction

In view of data security, people pay more and more attention to the construction of legal security prevention system, and have been widely concerned by various industries in society. Because of data security, it can not only involve the privacy of citizens' personal information, but also involve the maintenance of social public interests and national interests [1]. In the life cycle of data, hidden dangers in every link may endanger the security of data, such as illegal theft and over-collection during data collection, virus attack during data storage and processing, and association analysis and restoration attack during data use [2-3]. Whether it is departmental laws or regulations or local laws or regulations, their legal effect level is generally low, and their scope of application is also limited. There may be conflicting provisions among them, which are difficult to be used as the legal basis for the court to decide cases. Objectively, they directly affect the effective maintenance effect of data security [4-5]. The establishment of the basic law of maintaining data security needs to reflect the establishment of the basic principles of data security, the regulation of basic maintenance system and the formulation of the core content of maintaining data security. The formulation of other relevant laws and regulations needs to be extended based on such a basic law. That is to say, only by constructing such a basic law can the construction of China's legal system for maintaining data security become backbone [6]. Therefore, in the development of AI, every link in the data life cycle may cause the disclosure of state secrets, business secrets and personal information, thus

endangering personal privacy, social security and national security.

2. The Dilemma of Data Security Based on the Development of AI

The development of AI technology has brought tremendous technological progress to human society. AI technology is widely used in various scenes of life. Due to the outbreak of the epidemic, AI technology has been widely applied in epidemic prevention and control, such as facial recognition technology, temperature measurement technology, etc. [7]. The innovative development of AI mainly relies on deep learning, which involves collecting a large amount of data for simulation training, thereby promoting the accumulation of AI knowledge and experience and achieving intelligence. Traditional protection cannot meet the security needs of AI data [8]. Traditional protection systems rely on the pattern matching of existing known attack feature libraries and cannot identify unknown threats. Unknown threats hit once, making it difficult for traditional network security devices to cope with threats such as operating system vulnerabilities, application system vulnerabilities, database vulnerabilities, hardware chip vulnerabilities, and data sharing demand inflation. Frequently, there are accidents such as missing data usage logs, data breaches, security incidents that are difficult to trace, security incidents that are difficult to locate, inability to achieve proactive defense, and inability to proactively block risks. Therefore, this article constructs an AI data security attack model, as shown in Figure 1.

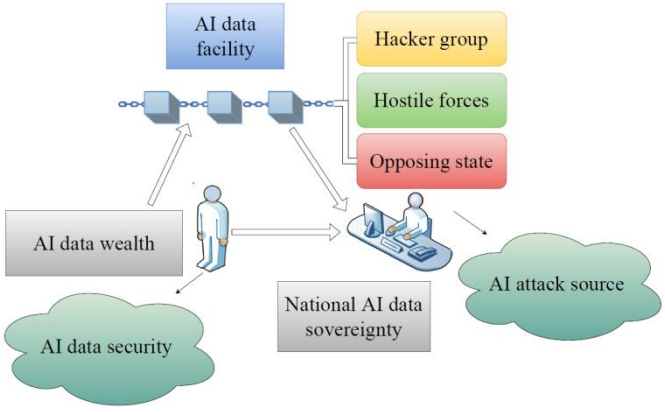

Figure 1: AI Data Security Attack Model Diagram

At present, in the construction of the legal system for maintaining network data security in China, there are relatively many local or departmental laws or regulations, accounting for the vast majority, while the basic laws or regulations promulgated at the national level are relatively few, accounting for a relatively low proportion [8]. With the use of AI in various scenes of life, providing a comprehensive and reasonable security guarantee system for data query security can effectively meet its various security needs, reduce the query security risks faced by data to as small as possible, and thus ensure the legal and reliable query of data [9]. AI technology can also be used to solve data security problems. In order to effectively solve this dilemma, interdisciplinary cooperation is needed, including professional knowledge in computer science, information security, law and ethics. In addition, policy makers, enterprises and society also need to work together to establish a strong legal framework, standards and ethics to maintain data security and privacy, while promoting the innovation and development of AI[10]. The problem of data security is outstanding, and China has accelerated legislation to protect the security of data in the development of AI at the legal level.

3. Current Status of Data Security Legislation

Boundaries should be established and norms established in the collection, storage, processing,

and use of personal information. However, the 'Principles' are only the framework and action guide for AI governance, lacking a certain degree of enforcement. In order to promote data empowerment, ensure data security in the process of AI development, and ensure the driving role of data in the development of the digital economy, China has formulated a corresponding legal system. Articles 1032 to 1038 of the Civil Code clarify the right to personal privacy, define personal information protection, and leave space and establish direction for the Personal Information Protection Law, which is included in this year's legislative agenda. The problems and deficiencies in legislation are mainly manifested in two aspects, as shown in Figure 2.

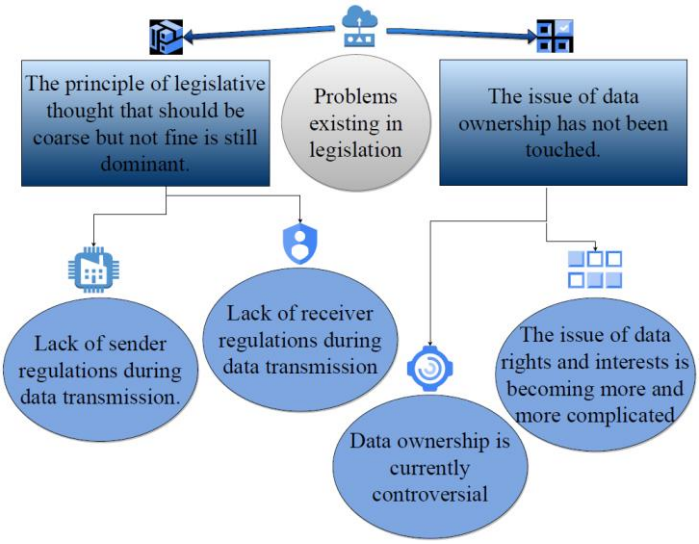

Figure 2: Legislative Issues

At present, China has established a basic law to maintain network data security, but some regulatory content is generally limited in length, with relatively vague regulations and a lack of operability. Other departments have relatively few regulations on computer system security protection, computer information network international internet management and security protection, internet information service management, computer information system security professional product testing and sales license management, and commercial password management. And international network security management or computer virus prevention and control management for computer information systems. On a global scale, countries and regions have formulated various laws and regulations to address data security challenges in different fields and industries. Enterprises and organizations need to closely monitor and comply with applicable regulations, while taking appropriate security measures to protect their data assets to ensure compliance and data security. In the future, data security legislation is expected to continue to evolve to address the challenges of emerging technologies and threats.

4. Legal guarantee promotes the accelerated development of AI data security technology

4.1. AI Data security policies and regulations promote the accelerated development of technology

After the formulation of the Basic Law on Network Data Security Protection, it is necessary to give necessary feedback on the implementation of the law. This requires the establishment of a feedback mechanism for the construction of network data security protection law. Relying on the feedback mechanism can effectively promote the implementation of the basic law of network data security. Through the inspection and supervision of the feedback mechanism, it is easy to find some

problems existing in the formulation of laws, thus laying the foundation for the subsequent legal revision work. Strengthening the legal protection of network data security risk prevention has become an important part of the overall work of network informatization. At present, the network data security problems that have occurred have had a serious impact on the social and economic construction and development in the new era. In the construction of level 3 and above information systems, encryption, active defense, auditing and other technologies should be adopted to protect data security. Ensure the data confidentiality requirements for the construction of level 3 and above information systems, and provide or support cloud tenants to deploy data security solutions. The strict implementation of industry laws and regulations has brought about the urgent need of the industry and accelerated its development. Industry laws and regulations, especially the management measures of information security level protection, have promoted the accelerated development of the industry.

4.2. The Cybersecurity Law of the People's Republic of China promotes the accelerated development of technology

The Cybersecurity Law of the People's Republic of China is an important regulation promulgated by the Chinese government in 2017, aimed at maintaining national cybersecurity and protecting the network rights and interests of citizens and organizations. This law not only emphasizes the importance of cybersecurity, but also to some extent promotes the accelerated development of technology. There is no clear definition of ownership of data assets in existing legislation, and there is controversy over this understanding among data subjects, data processors, or data controllers. Personal data rights include property rights and personal rights, and the ownership of data determines the distribution of data value and benefits, as well as the division of responsibility for data quality and security. Individuals have absolute rights to data property, but there are also opposing opinions. Some people believe that in the era of AI or big data, the value of personal data needs to be discussed, and data controllers or platforms use a large amount of collected data to create value. Therefore, the ownership data controller. In the lifecycle of data, every hidden danger in every stage may endanger the security of data, such as illegal theft and excessive collection during data collection, virus attacks during data storage and processing, association analysis and restoration attacks during data usage. The Cybersecurity Law of the People's Republic of China provides a solid legal framework for China's cybersecurity environment, while also promoting technological research and innovation. By strengthening data protection, threat response, and international cooperation, this law helps to improve the level of network security, protect user privacy and data. At the same time, it has also promoted the development of network security technology and provided strong support for China's position in the global network security field. However, the specific implementation and regulation of the law still require continuous attention and improvement to ensure its effectiveness and adaptability.

5. Conclusions

In this paper, data security risks and legal research are considered and analyzed in the AI era. In view of the new problems in the field of information security, under the guidance of the principle of unification and consistency with the basic law of information security, the national information security functional department can formulate relevant departmental rules in advance and raise them to administrative regulations or laws as soon as the time is ripe. The threats and demands of AI data security and legal protection have jointly promoted the great development of AI data security technology. The threat and demand of AI data security is the first driving force for the development of AI data security technology, and legal protection promotes the accelerated development of AI

data security technology. Through legislation, the right of network transmission has been added to protect the rights of traditional works on the network and the copyright of online works, so that all original intellectual achievements can obtain corresponding legal status and legal protection. At the same time, the legal license on the internet has been liberalized, which makes the online information spread more quickly. Combined with security technology, we can severely crack down on those behaviors that endanger the security of network data, so as to protect the security of network data and provide necessary legal guarantee for protecting people's property. Forecast the possible network security threats and attacks in the future; At the same time, various technologies are comprehensively utilized to assist in the analysis, judgment, disposal, response and countermeasures of network security threats.

References

[1] Rakowski R, Polak P, Kowalikova P. Ethical Aspects of the Impact of AI: the Status of Humans in the Era of Artificial Intelligence [J].Society, 2021, 25(14):18-25.

[2] Han S, Han K, Zhang S.A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era[J].IEEE Access, 2019, 30(10):10-22.

[3] Dongmei X, Lige T.EU data protection impact assessment and its implications[J].Journal of Library Science in China, 2018, 33(10):41-49.

[4] Abbas A.AI & Racial Equity: Understanding Sentiment Analysis Artificial Intelligence, Data Security, and Systemic Theory in Criminal Justice Systems [J]. 2022, 28(11):48-55.

[5] Xu W, Nie Y. Research on the Legal Protection of Personal Information Security in the Era of Big Data[J].Journal of Physics: Conference Series, 2020, 1648(3):032067-032074.

[6] Zhang Y, Ma Z, Luo S, et al. DBSDS: A dual-blockchain security data sharing model with supervision and privacy-protection [J].Concurrency and computation: practice and experience, 2023, 22(7):36-42.

[7] Deng X, Zhang B. Research on Legal Protection System of Personal Information in Big Data Era[J].IOP Conference Series: Materials Science and Engineering, 2020, 806(1):012032-012039

[8] Wang Z. Personal Information Security Risks and Legal Prevention from the Perspective of Network Security[J]. Springer Books, 2020, 18(4):12-17.

[9] Hallur G G, Prabhu S, Aslekar A. Entertainment in Era of AI, Big Data & IoT[J].Springer Books, 2021, 12(7):10-15.

[10] Vockley M. Articles About AI, Cybersecurity, and Alarm System Safety Recognized with AAMI Award[J].AAMI news: Association for the Advancement of Medical Instrumentation news, 2023, 11(4):17-22.