Scientific and Social Research, 2024, Volume 6, Issue 10
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Analysis of Personal Privacy Leakage under the Background of Digital Twin

Leyi Zhang, Jingguo Xue*

Beijing University of Civil Engineering and Architecture, Beijing 102627, China

Corresponding author: Jingguo Xue, xuejingguo@bucea.edu.cn

Abstract: With the development and application of digital twin technology, the problem of privacy leakage is becoming increasingly prominent. Privacy leakage issues caused by data abuse and weak awareness have attracted high attention. In this regard, this paper analyzes the causes of privacy leakage in the digital twin, analyzes the difficulties of privacy protection under the background of the digital twin, and puts forward the "legal co-governance model." Through multi-party cooperation, improving the system, and improving literacy, people can effectively protect private information, ensure the security application of technology, law, and ethics, and provide a guarantee for the sustainable development and social application of digital twin technology.

Keywords: Digital twin; Privacy leakage; Privacy protection; Legal co-governance model

Online publication: November 5, 2024

1. Introduction

The current construction of digital China has stepped into the "digital twin era." Digital space is realizing the replication or even surpassing of real space, and digital projects such as smart transportation, smart cities, and smart courts are emerging in an endless stream [1]. However, with the expansion of the application scope of the digital twin, its decision needs to be supplemented by a large amount of information data such as personal identity, living habits, and property situation. This sensitive information is an important support for the development of the digital twin era, but it also brings the risk of personal privacy leakage. The privacy information of the collected person is often leaked, and it is even applied to illegal and criminal activities. Therefore, how to effectively protect personal privacy in promoting the development of digital twins has become a common challenge facing the industry.

Given this problem, some scholars point out that people should accelerate the construction of digital twin ethics and build a virtual and real community [2]. Some scholars have proposed that data protection and privacy needs should be met [3]. However, digital twin technology is still in the development stage, and China has not

established perfect laws and regulations and clear ethical standards, and it is difficult to prevent the behavior of leaking personal privacy information. The main reason is not to "apply the right medicine", that is, only using the general method to solve similar problems, but not to further explore the root cause of privacy leakage. Privacy protection in digital twins requires comprehensive consideration of technology, law, and ethics, which is a complex structural problem. The prescription to solve the total problem is not only limited to solving the original problems but also easy to produce new risks. In this regard, this paper will analyze the reasons for personal privacy leakage under the background of digital twins, and further explore the protection path.

2. The cause of privacy leakage in digital twins

With the development and progress of digital twin technology, the wide application of big data, 5G, and other technologies, the collection and disclosure of user personal information for benefits are endless. Even though China has gradually formed a legal system based on the Civil Code, the Personal Information Protection Law as the core, the Network Security Law, the Data Security Law, and other regulations and regulations as the guarantee, 800 million people around the world are still suffering from chaos such as data abuse [4]. The causes of privacy leakage such as data abuse can be divided into two categories according to the system boundary standard, namely, the privacy leakage caused by external and internal causes.

2.1. Privacy leakage caused by big data and other external causes

According to the 2023 Annual Report on Data Leak Risk in 2023, among the nearly 150 million pieces of intelligence monitored by the data leakage risk monitoring platform in 2023, more than 19,500 data leakage incidents were analyzed and verified [5]. The complexity and black box characteristics of big data analysis algorithms (opacity) make personal privacy data more vulnerable to invasion, and the lack of a clear imputation system also further aggravates the possibility of privacy leakage.

2.1.1. Data abuse

Digital twins rely on collecting and processing real-world data information to build databases. Among them, in the data processing process, personal information is often used for illegal activities and sold to unauthorized third-party commercial promotion. In 2023, "citizens' personal information" will still be the main type of data abuse, accounting for more than 90%. With the adoption of digital twins, experts predict further data abuse by 2024.

2.1.2. Algorithmic black box

Digital twins construct the real world in digital space, and data-driven algorithms make decisions and pass them to the real world through the interface. However, the operation logic of the digital space —— the algorithm is opaque, and it is difficult for users to understand the logic or decision-making mechanism within the algorithm, which is vividly described as a "black box." According to the China Big Security Perception Report (2021), 70 percent of respondents are concerned about their personal privacy [6]. These concerns are not raised on a whim, let alone out of thin air. Personalized recommendation by social media is the behavior that uses users' personal information and behavioral data to adjust decision rules and influence users' opinions. The opacity of algorithms and the uncontrollable flow of private data are increasing the risk of personal privacy.

2.1.3. Perspectives

In the digital twin, the liability vulnerability of privacy leakage mainly comes from the problem of algorithm black box, and it is particularly difficult to investigate the responsibility of algorithm technology. This has once become a research hotspot in the academic circle —— algorithm technology is not transparent, which leads to criticism. In the algorithm black box, the process of infringing the privacy right is complex and systematic. To make a more systematic study, considering that the digital twin technology is still in the development stage, according to the judgment concept of similar cases, the author searched "privacy" and "big data" in the research database of Peking University, and found a total of 373 related cases. After the summary, the four examples with the highest correlation were analyzed, summarized, and detailed in **Table 1**.

Table 1. Examples of cases involving misusing privacy leakage

Related Cases	Infringer	Infringee	Facts of damage	Principle of evidence
Chen v. Hangzhou Software Service Co., Ltd. Network Service Contract Dispute Case - Judicial Determination of Traffic Hijacking, User Cookie Record Privacy, and Evidence Disclosure	Company A	Mr.Chen	Company A freezes Chen's platform promotion account	Fault liability principle
Pang Lipeng v. China Eastern Airlines Co., Ltd. and Beijing Quna Information Technology Co., Ltd. Privacy Dispute Case [7]	China Eastern Airlines and Quna Company	Pang Lipeng	Leakage of Pang Lipeng's information, including name, phone number ending in * * 49, itinerary, etc	The inverted burden of proof
Unfair Competition Dispute Case between Beijing Weibo Vision Technology Co., Ltd., Shanghai Liujie Information Technology Co., Ltd., Xiamen Waist Muscle Network Technology Co., Ltd., and Zhejiang Taobao Network Co., Ltd	Liujie Company	WeChat broadcasting company, "Tiktok" anchors and rewards users	Illegal acquisition of non-public data such as Tiktok platform users' live broadcast reward records (specific to each user's reward time, object, and amount) and anchor reward income-related data (including anchor's single play, daily, monthly, and annual income), and public display after self-sorting and calculation [8]	Fault liability principle
Case of Li et al. infringing on citizens' personal information, Wu Jian et al. provide intrusion and illegal control of computer information system programs and tools.	Li Jin, Gong Wenhui, Wu Jian, Zhang Zhuo	Customers of Taobao merchants	Illegally obtaining customer data from merchants (including customer names, contact information, mailing addresses, etc.) totaling over 730000 yuan.	Fault liability principle

As can be seen from the above table, there are the majority infringement of big data infringement cases and multiple infringed cases, and the burden of proof has different application rules in different infringement cases. Similar to the black box of the digital twins algorithm, which also involves multiple objects. The complexity of the tort subject makes it difficult to identify subjective fault, which increases the difficulty of identifying tort liability in digital space. The diversity of infringement objects and the concealment and unpredictability of infringement also increase the difficulty of determining the facts of infringement. In addition, China's existing laws and regulations do not clearly stipulate the accountability principle of digital space, and the "safe haven principle" has become an excuse for digital space, which further aggravates the possibility of privacy leakage.

2.2. privacy leakage caused by public awareness

In addition to privacy leakage caused by big data and other external causes, citizens' weak awareness is an important internal cause of privacy leakage. A survey and interview of 1,036 people conducted by a research team at Wuhan University found that 77.8% of users "rarely or never read the privacy protocol" when installing the application, and 69.69% would ignore the update tips of the app privacy protocol [9]. This is like voluntarily giving up their privacy rights. In the digital age, people often show a weak awareness when facing personal data security and privacy protection, and sensitive information is easy to leak. Through sensitive information, criminals can easily analyze the portrait of specific natural persons and even predict the psychology and behavior of specific natural persons, and then carry out criminal activities [10].

3. The contradiction of privacy protection in the context of digital twins

The development of digital twins brings new challenges and risks to personal privacy, but the protection of personal privacy may limit the development and application of digital twins. Large-scale data analysis and processing is the core of digital twin technology, but improper use or disclosure of personal privacy data will violate personal privacy.

Therefore, although digital twins technology needs a large amount of data to support its development, more attention must be paid to privacy protection in the process of data collection to ensure the legitimacy, transparency, and security of data collection. In this context, corresponding policies and regulations need to be explored and formulated to ensure that user privacy is fully respected and protected and to promote the healthy development and rational use of digital twin technology.

4. The protection path of privacy in the background of digital twin rights

To solve the problem of privacy leakage in digital twins, the author puts forward the legal co-governance model based on the reasons for privacy leakage (**Figure 1**). Comprehensive use of law, system, and literacy tripartite path, to promote the healthy development of digital technology, while maximizing the protection of personal privacy and security, to build a more secure and reliable digital twin environment.

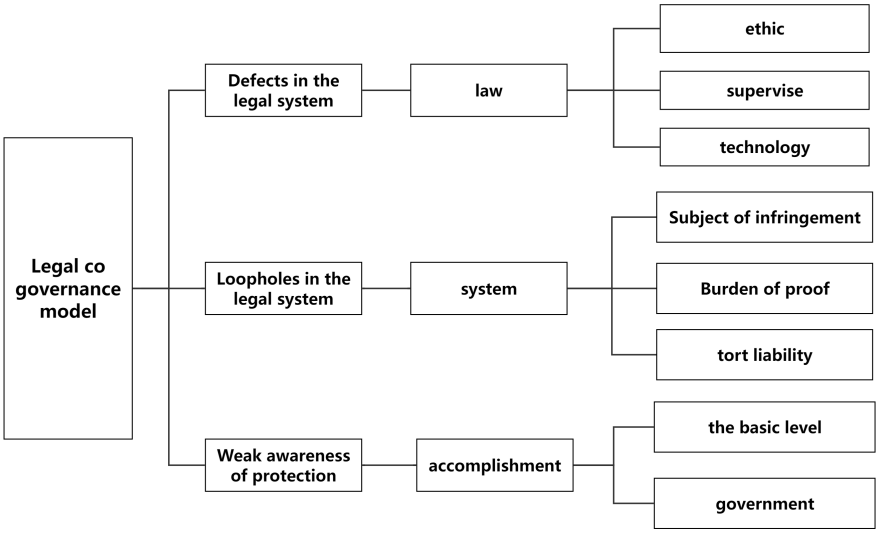

Figure 1. Legal co-governance model

4.1. Agglomeration force and joint governance

The protection of privacy under the background of digital twins needs to gather the forces of the country, society, and individuals to play a coordinated role. At the national level, a national information resource sharing system should be established, the legislation should be improved, the rules for assuming tort liability should be clarified, and the complementarity between law and ethics, mutual assistance between law and supervision, and mutual cooperation between law and technology should be realized. At the social level, the public should be encouraged to participate in data security governance, and digital twin research and development enterprises should be encouraged to enhance their autonomy and assume social responsibilities. At the same time, the public also needs to strengthen their awareness of their privacy data prevention.

4.1.1. Law and ethics are complementary

Ethics and law are two important concepts and practical fields in the development of human society. Ethics is based on human values and morality and explores the norms of human behavior. The law is a mandatory norm approved by the state. Together, they shape social morality and the normative system. Therefore, the combination of ethical guidance and legal governance can play a dual role in the public in today's society [11].

In 2022, China issued the Opinions on Strengthening the Governance of Science and Technology Ethics, which provides a top-level design for solving problems such as the imperfect governance system of science and technology ethics, but the data ethics norms in subdivided fields need to be further improved. In this regard, people can refer to the Business Data Ethics Framework released by the United States in March 2023 to further clarify the specific principles of privacy, confidentiality, transparency, accountability, and credibility contained in China's data ethics system, to build a strong national framework for the protection of personal data.

4.1.2. Mutual assistance between law and supervision

Digital twin technology needs to clarify the regulatory subject, regulatory content, and regulatory responsibilities with the help of legal regulation. In terms of clarifying the regulatory subject, it is suggested that the government should establish an independent third-party organization under the government, and the credibility of the government should supervise the digital twin application, and ensure that the division of responsibilities under the "Internet +" mode, to improve the effectiveness of regulatory implementation [12]. In addition, the public and the relevant media should also participate in the supervision to realize the coordinated supervision of multiple subjects.

The regulatory content should include standardized evaluation, information leakage, and other aspects. With the help of the "penetrating" supervision mode, the connection point between data security risks and legal norms can be found through technical means, and the risk prevention mechanism can be established by law. At the same time, regulatory data should be disclosed within the legal limits to improve the quality of supervision and promote the deep integration of digital twins and market demand.

In addition, a digital twin technology accountability and error correction mechanism should be established to timely trace the existing problems, and publicize the evaluation results, to encourage supervisors to fulfill their supervision responsibilities, and those who cannot timely rectify should be investigated accordingly.

4.1.3. Interaction between law and technology

Advanced technology support is a necessary condition for digital twin risk prevention and control. It is

suggested to embed the risk prompt function in the digital twin project, build the early warning mechanism of the "black box" of the digital twin algorithm, and include it in the regulations to strengthen the behavior supervision and risk control of the digital space. Once the algorithm is found, the warning function is activated and the transparency of the algorithm is evaluated, to promote the realization of "visual justice" of the algorithm and further prevent and control the leakage of personal privacy data [13].

4.2. Improve the tort liability system

Although China has not issued special digital twin laws, it is very important to improve the responsibility system in legislation, especially for the risk of data leakage. To protect personal privacy and data security, the system attacker, as a subjective intention, should apply the fault liability principle to bear the main legal liability. At the same time, for the system developers and users, if they cannot prove that they have carried out the necessary risk prevention and control work, they can be presumed to bear certain liability for negligence. In general, for the infringed, due to the risk of black box, the principle of reversing the burden of proof should be adopted at necessary times to reduce the burden of proof of the infringed.

A sound responsibility system not only provides the necessary policy basis for accountability but also warns the developers and users to fulfill the necessary data protection obligations. Through the diversification of responsibility risks, promote the establishment of a sound twin data leakage responsibility system, and further protect the legitimate rights and interests of the public.

4.3. Improving public legal literacy

The digitization process is accelerating, and the public also pays more attention to privacy protection awareness. However, according to the 2019 Research Report on The Information Security of Chinese Netizens, 47.5% of netizens who have suffered from private information disclosure are ignored [14]. Although the public has a certain awareness of privacy protection, there is still a large passive attitude in practical action. Therefore, while strengthening the public awareness of privacy protection, officials should also turn passivity into initiative and encourage the public to actively maintain personal privacy information.

From the perspective of grassroots, the community neighborhood committee should play its functions, make public welfare slogans about privacy protection, and put them on the community publicity board to spread the theoretical knowledge of privacy protection to the community citizens, through knowledge contests and setting up personal privacy protection consultation, strengthen the awareness of privacy protection in practice. From both concept and practice, citizens are encouraged to maintain personal privacy information. For individuals, whether it is a small program to apply for permission or signing a contract involving multiple information, each clause should be read carefully, especially the important provisions concerning personal privacy and information [15].

The government should strengthen public participation in the digital space and ensure the maximum right to know and the right to make suggestions. As an end-user and beneficiary of the digital twin, the public has the right to understand how the data is collected and used, and the potential risks and benefits that may arise. In the process of policy formulation and technology application, the public should be encouraged to actively participate, collect and listen to opinions from various parties, and ensure that the development of digital twin technology meets the expectations and needs of the public.

5. Conclusion

As an emerging technology, the application of digital twin applications faces privacy leakage as one of the drawbacks. For the privacy leakage problems caused by data abuse and weak public awareness, officials can combine law, ethics, supervision, and technology to work together to improve the tort liability system and improve public legal literacy. When the privacy issue is effectively regulated, the digital twin technology can better serve social development and human well-being.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Yi JL, 2021, Law and Accountability in the Digital Twins Era —— Through the Technical Standard Perspective Algorithm Black Box. Oriental Law, 2021(4): 77–92. https://doi.org/10.3969/j.issn.1007-1466.2021.04.007

[2] Diao SF, Kong XY, 2022, Ethical Issues on the Application of Digital Twin Technologies in the Educational Field. Journal of South China University of Technology (Social Science Edition), 24(06): 16–24. https://doi.org/10.19366/j.cnki.1009-055X. 2022.06. 003

[3] Beduschi A, 2019, Digital Identity: Contemporary Challenges for Data Protection, Privacy and non-discrimination Rights. Big Data Society, 6(2): 205395171985509.

[4] Shi ZY, Jin C, 2024, The Institutionalization of Digital Ecological Civilization: The Implication of the Time, the Development Dilemma and the Game-breaking Strategy. Journal of China University of Geosciences (Social Science Edition), 24(2): 117–130. https://doi.org/10.16493/j.cnki.42-1627/c.20240015.001

[5] Threat Hunter, 2024, 2023 Data Breach Risk Annual Report, https://www.threathunter.cn/blog/2023-30a8268f-be39-4e6e-91cb-2e5b97a4780f

[6] Meng FZ, 2023, Strengthen Co-governance, Standardize the Application and Development of Algorithms. The China Press Industry, 2023(09): 5. https://doi.org/10.13854/j.cnki.cni.2023.09.109

[7] Zhai JG, Zhang XL, 2020, Application Guidelines and Typical Case Analysis of the Civil Code of the Peoples Republic of China. China Democracy and Legal System Publishing House, Beijing.

[8] Zhao D, Shen C, 2023, Investigation and Reflection of the Judicial Review Elements of Data Capture and Unfair Competition Disputes. Technology and Law (Chinese and English), 2023(2): 52–59.

[9] Yuan K, Zhang SH, Ma SS, et al., 2021, The “Right Book” to Guarantee Security is still the “Arbitrary Door” to Steal Information. Guangming Daily, August 19, 2021, 7. https://doi.org/10.28273/n.cnki.ngmrb.2021.004263

[10] Cai BK, Xu XL, 2023, Legal Regulation Analysis of Data Security in the Application of Artificial Intelligence. Technology Think Tank, 2023(07): 45–52. https://doi.org/10.19881/j.cnki.1006-3676.2023.07.07

[11] Xu RP, Liu J, 2022, Algorithmic Risk and Ethical Governance in the Digital Twins Era. Journal of Foshan University of Science and Technology (Social Science Edition), 40(04): 31–39. https://doi.org/10.13797/j.cnki.jfosu.1008-018x.2022.0037

[12] Zhang M, Zhang N, 2022, The Legal Dilemma and the Perfect Path of the Intelligent Pension. Journal of Yuncheng College, 40(02): 53–60. https://doi.org/10.15967/j.cnki.cn14-1316/g4.2022.02.004

[13] Yan Q, 2022, Digital Twins: Risk, Traceability, and Regulation. The National Library Academic Journal, 31(05): 104–112. https://doi.org/10.13666/j.cnki.jnlc.2022.0511

[14] Li HR, Wang ZB, 2021, Research on Personal Information Protection of Government App under the Background of Reform of "Decentralization, Administration and Service". Information Network Security, 2021(S1): 45–49.

[15] Wang LP, 2022, Privacy Regulation in the Context of Artificial Intelligence. Network Security Technology and Application, 2022(08): 124–126.