Research on Legal Protection of Big Data Privacy Security

Xianyang Cheng[1a] , Yun Gao[2b]

{chengmo03298011@163.com[a], yg52s@login.missouristate.edu[b]}

[1]Low School LiaoNing Normal University, Dalian, Liaoning, China, 116082,
[2]LNU-MSU College of International Business, Dalian, Liaoning, China, 116000

Abstract. With the rise of the Internet era, the use of big data has become widespread. However, with the convenience it brings, the privacy and security concerns regarding big data have become increasingly apparent. This paper aims to provide an overview of the current state of laws and regulations on big data privacy and security in China. It will analyze the existing problems such as limited theoretical research, an imperfect legislative system, ambiguous powers and responsibilities of relevant institutions, and inadequate judicial remedies. Additionally, a series of measures will be proposed to address these issues, including the improvement of relevant legislation, the strengthening of supervision measures, and enhancement of judicial relief. These efforts aim to effectively enhance the protection of big data privacy and security in China.

Keywords: big data environment; privacy security; legal protection

1 Introduction

The era of big data is a contemporary era that encompasses not only technological advancements but also significant changes in social life. In today's world, data has become the key driver of competitiveness and resource sharing. Safeguarding and effectively utilizing data resources have become crucial in the digital economy era[1]. The application of big data has greatly enhanced the convenience of people's lives, enabling the quick and accurate matching of valuable information based on personal preferences and needs. However, this convenience also presents a challenge in the form of privacy breaches. Instances of privacy breaches have been uncovered worldwide, such as the revelations made by CIA employee Snowden regarding the "Prism Project" in the United States and the leakage of account registration information and email addresses of over 20 million users on a Russian social networking site. According to a survey report on the rights and interests of Chinese netizens released by the Internet Society of China, there are over 1.5 million individuals involved in the illegal industry of profiting from selling other people's private information and data in China. In just two years, personal privacy data has been leaked a staggering 6.5 billion times, resulting in economic losses of approximately 91.47 billion yuan. This has serious implications for the stability of the Internet economy and even society as a whole. China has been increasingly emphasizing the protection of data privacy over the years, implementing improvements in relevant legislation, and developing laws and regulations that are suitable for the national context.

ICPDI 2023, September 01-03, Chongqing, People's Republic of China

DOI 10.4108/eai.1-9-2023.2338759

Additionally, China is actively building a data privacy security protection system that reflects the unique characteristics of the country[2].

2 Concept and Present Situation of Data Privacy

2.1 The Concept of Data Privacy

In China, the concept of privacy, known as "privacy," has existed since ancient times. Its origins can be traced back to Han Shu, where it referred to hidden matters. However, the theory of privacy in the legal field emerged much later, towards the end of the 19th century, thanks to American judge Thomas Cooley. In China, the earliest provisions relating to privacy were introduced in 1988 through "The Supreme People's Court's Decision on Implementing Article 140 of Opinions on Several Issues of General Principles of Civil Law of the People's Republic of China (Trial)." This decision relied on the right of reputation to safeguard privacy. Presently, Article 1032, paragraph 2, of the Civil Code definitively outlines the concept of privacy: it comprises the peaceful private life of individuals, as well as private space, activities, and information that one does not wish to share with others. Building upon this foundation, the right to privacy in the era of big data has acquired new dimensions. In 2012, the European Union introduced the General Rules for Data Protection. Chapter III, Volume III, Paragraph 17 of these rules mentioned the right to be forgotten and the right to be deleted. This means individuals have the right to have their data removed from databases managed by information data collection managers. They also have the right to prevent the further dissemination of this data. It is important to note that when the data subject is a young child, it is even more crucial to give them the power to make decisions regarding their personal information. Essentially, this is about individuals' right to control their own privacy, which involves conflicting value goals among different parties. In today's world, where privacy protection and privacy infringement are in conflict, there are significant challenges in finding better ways to safeguard privacy[3]. The power of AI can be harnessed for economic gain in ways that are harmful to individuals and society: users, consumers, and workers may be subject to pervasive surveillance, controlled in their access to information and opportunities, and manipulated in their choices.[4]People's actions are constantly under digital surveillance, which is causing a significant reduction in individual privacy. This poses a growing contradiction with individual freedom.

2.2 Status of Data Privacy Protection

Currently, the right to privacy in China is primarily addressed in the following areas: firstly, the protection of citizens' personal information and public interests; secondly, the guarantee of citizens' freedom of communication; thirdly, the balance between confidentiality privilege and the boundaries of private space; and fourthly, the safeguarding of personal peace, privacy, and related rights. When considering big data, there are also concerns regarding the right to access information about big data and private correspondence, which fall within the legally defined scope of privacy. Despite the absence of specific privacy or data protection laws in China, various laws and regulations still incorporate provisions for privacy protection. These laws and regulations have been collected and organized to form the existing framework for privacy protection in China.

Table 1 Laws related to data privacy security [5]

Abbreviation/full name	Main clauses related to data privacy governance
《Constitution》	Articles 38-40
《Penal Code》	Articles 245, 246, 252 and 253 bis
《Civil Code》	Articles 110, 111, 127, 1032-1039
《Cyber security law》	Articles 10, 12, 21-22, 27, 40-50, 59-60, 64, 68, 70
《Criminal Procedure Law》	Articles 54, 152, 188
《Civil procedure law》	Articles 68, 134, 156
《Statistical law》	Articles 54, 152, 188
《Electronic commerce law》	Articles 5, 23, 25, 32, 79, 87
《Law on Public Security Administration Punishment》	Articles 42, 80
《Law on the Protection of Minors》	Articles 39, 58, 60 — 63
《Basic Medical Care and Health Promotion Act》	Articles 33, 92, 102, 105
《Data security law》	Articles 8, 29, 42
《Personal information protection law》	Articles 2, 21-24, 29, 31-32, 34, 36, 38-40, 44-52

Law is not only the most powerful weapon but also the most solid guarantee for controlling data privacy. Currently, China is placing a greater emphasis on data privacy security. It is of utmost importance to identify the existing problems and delve deeper into the development path of data privacy.

3 Existing problems of data privacy

3.1 Fewer relevant studies

Theory is the precursor to practice. Currently, the strengthening of privacy protection in our country needs to be further addressed from a theoretical standpoint. China has adopted the principle of "taking facts as the basis, taking laws as the criterion" and "having laws to follow" for personal information protection. However, with the constant development of Internet technology, new technologies continue to emerge, posing serious challenges to various issues such as defining the scope of traditional privacy rights, inevitably leading to privacy disputes. Given the evolving lifestyles and increasing reliance on the Internet, it is crucial to thoroughly analyze various measures to prevent violations of citizens' rights and interests in theory during today's era of big data. Consequently, data security and privacy protection should be considered as pivotal aspects within the legislative field, leading to the advancement and enhancement of theoretical research.

3.2 The systematization of laws and regulations is imperfect

As for the right to privacy, As shown in Table 1, at present, our country's privacy protection system is scattered between various laws and regulations, and there is no special protection.

China's Civil Code addresses its concept from a broader perspective. It mainly focuses on protecting personality rights and interests. However, the current approach to this protection work is somewhat limited and narrow, primarily aiming to prevent the violation of human dignity[6]. In the context of big data, it is necessary to "upgrade" the corresponding privacy content, as the traditional privacy rights alone are insufficient to address the challenges of the big data era. In our country, personal information security and personal privacy have often been overlooked, with attention only given to network security and implementing measures to ensure a secure online environment free from hackers. However, the protection of citizens' personal privacy has been neglected[7] .[Due to the absence of adequate system guarantees and effective supervision and regulation of internet usage by citizens, criminals exploit existing loopholes to infringe upon the legitimate rights and interests of others, disrupt social public order and even compromise national security. They acquire personal information or trade secrets through unfair competition methods, resulting in the disruption of the socialist market economy. This situation also poses a significant challenge to China's market regulation and has far-reaching negative consequences.

Therefore, it is crucial for the law to accurately define and protect the right to privacy. In the current age of big data and the information society, the reach of the internet expands globally, allowing us to access a vast amount of information from all over the world. This presents a unique challenge as all types of information are readily available and shared on open platforms. Consequently, it is imperative that privacy rights are safeguarded to ensure responsible usage and dissemination of online information. Secondly, people's limited awareness of protecting the right to privacy on the Internet results in frequent and increasing infringements. Furthermore, due to imperfect legislation, a significant number of cases involving reputation rights and privacy rights cannot be adequately protected, and the boundaries regarding privacy rights are undefined. Consequently, our citizens lack a precise understanding of the concept of privacy. Thus, it is essential to define the privacy rights enjoyed by citizens within the context of big data.

3.3 The powers and responsibilities of relevant institutions are not clearly defined

In the big data environment, the absence of specific rules and regulations for privacy protection results in an imperfect implementation system, unclear distribution of powers and responsibilities among law enforcement agencies, and challenging implementation. Additionally, the supervision and implementation of the law must be conducted concurrently. During the process of legislation, law enforcement, and judiciary, it is essential to involve the supervision of relevant functional departments [8]. Currently, China does not have a dedicated regulatory agency for privacy protection, and the inadequate regulatory mechanism results in frequent ineffective supervision. In the case of multi-head supervision, different departments operate independently without proper communication, avoiding responsibilities and shirking each other. This results in frequent instances of lack of supervision, conflicts of power, and other undesirable phenomena. Consequently, the overall efficiency of government agencies is greatly reduced, administrative resources are wasted, and the underlying issues are not effectively resolved[9] .Especially in the realm of network supervision, privacy invasion poses a significant challenge due to its rampant and rapid circulation. This issue has become a breeding ground for abuse of personal information via the internet. Unfortunately, the lack of dedicated law enforcement agencies or their negligence in taking responsibility hinders the effective implementation of privacy protection measures. Consequently, criminals take advantage of the vast data pool, leading to grave violations of citizens' privacy rights.

3.4The way of judicial relief is imperfect

Traditional methods are no longer sufficient to address privacy infringements in the era of big data. The concealment of the Internet makes it difficult to identify and promptly take appropriate measures against new infringement methods, often resulting in significant damage. Additionally, the wide geographical reach makes it challenging to pursue litigation in the usual manner. Moreover, the litigation process is burdensome, time-consuming, and lacks timeliness, resulting in minimal impact. Despite the establishment of a representative litigation system in China, it is rarely witnessed in practice, with only a few cases being accepted by the court.

Secondly, the post-event remedies for privacy breaches in the context of big data are flawed. While there are numerous provisions for such remedies, the lenient punishments imposed on infringers in judicial practice result in repeated violations driven by the allure of personal gain, leading to frequent privacy breaches. When such a tort occurs, the protection of the affected individuals still requires improvement, and there is a lack of effective means to seek redress for violations of one's personal rights or property. These shortcomings, coupled with delayed relief, have contributed to a decline in the credibility of privacy protection in China, consequently diminishing the effectiveness of privacy safeguards within the realm of big data.

4 Legal protection path of data privacy

4.1 Improve relevant legislation

The era of big data networks has significantly increased the risk of personal information security, making it easier to leak personal privacy[10]. It is crucial to establish a comprehensive and effective personal information protection system. Firstly, the right to be forgotten should be granted appropriate legal status. As one of the most important privacy rights in the era of big data, giving it legal status contributes to the advancement and refinement of the overall legal protection system for privacy rights. With the rapid dissemination of big data, personal privacy can quickly spread far and wide. Simultaneously, due to the lasting presence of speeches, photos, and images published on the internet, regardless of their quality, they cannot be completely erased. Citizens suffer from the inability to fully erase this information, which hinders personal growth and prolongs societal memory. Additionally, certain shameful privacy instances are challenging to be forgiven by society. Therefore, it is crucial to incorporate the right to be forgotten into the existing legal framework. Granting citizens the ability to demand the deletion of personal information stored in big data carries significant importance in preserving the network environment, safeguarding personal privacy, and upholding individual rights. Building a privacy protection system with Chinese characteristics, centered around the right to be forgotten, is one of the key objectives of our legislation.

4.2 The Privacy Law was promulgated to stabilize the right protection of data privacy

Our country has enacted the Privacy Law as a distinct code, which can provide effective legal provisions for data privacy processing within our borders. Presently, despite China mentioning privacy protection in 21 laws and regulations, it lags behind developed nations like the United States, where privacy is ingrained in both federal and state legal systems. The United States Congress has passed various laws, such as the Communication Law (1934) and Privacy Law (1974), establishing a comprehensive personal information data protection system. When formulating China's Privacy Law, it is imperative to refer to the privacy legal framework of developed countries. Furthermore, while considering our specific national circumstances, we must prioritize striking a balance between personal information protection and internet development. Simultaneously, we must also achieve a balance between individual rights and public interests. Secondly, special provisions in the privacy law should address the controversial, problematic, and complex aspects of privacy that exist in theoretical and practical circles. These provisions should cover the constituent elements of privacy, the varying degrees of recognition for different types of privacy, and the different methods used to protect privacy in various situations. Additionally, we need to consider whether the level of privacy protection should differ for individuals engaging in the same behavior or different behaviors. This differentiation should be incorporated into legislation. For instance, in terms of online activities, individuals should have the right to inform data service operators when collecting their data, as well as the right for the data service operator to securely store their data. Based on this foundation, tort liability needs to be clarified, and the methods of assuming liability and providing relief should be further categorized. For instance, when violating the privacy rights of others' property and personal interests, liability should not only involve compensation for emotional harm, but also cover economic losses that can be accurately calculated. Additionally, the matter of jurisdiction warrants careful consideration. As mentioned earlier, jurisdiction is a significant and arduous matter in the era of big data, therefore, the Privacy Law should establish clear provisions regarding the jurisdiction of privacy violation cases. The author believes that online litigation has become widespread in our country, thanks to the continuous improvement of our intelligent judicial construction. Currently, it has been implemented in 3,500 courts, allowing big data privacy cases to be conducted in online court sessions based on their specific characteristics. Additionally, smart courts require innovative technical methods to effectively manage personal information, thereby strengthening the capability of judicial big data to support judicial practice[11].

4.3 Strengthen the supervision of privacy protection

China's Internet Information Office may establish a dedicated department for privacy protection and supervision. The authorities have greater responsibility in establishing collection and processing and personal data analysis systems, which should include privacy protection. This department will conduct periodic checks on the private information of citizens stored by enterprises.[12]In case of any violations detected, the department will issue warnings and orders for rectification. In more severe cases, appropriate punishments will be imposed.

Secondly, establish an annual evaluation mechanism for creating a white list and black list. Operators who prioritize and safeguard personal privacy throughout their operations will undergo screening and be included in the white list for recognition and public commendation. Conversely, the ten operators with inadequate measures will be blacklisted, their data information disclosure system will be temporarily shut down for five working days, and they will face economic penalties.

Finally, China can learn from the remarkable successes of the protection approach in Britain and New Zealand, and contemplate establishing a privacy protection specialist as a dedicated agency to oversee the privacy safeguarding of operators within the big data environment. This will enable us to define the law enforcement agencies responsible for privacy protection and their primary responsibilities.

4.4 Improve the judicial relief channels

The importance of the relief mechanism as the final line of defense in ensuring judicial protection is clear. A well-established and integrated judicial relief mechanism can enhance the effectiveness of safeguarding data privacy to some degree.

First of all, in the era of big data, the infringement of data privacy is a common behavior that results in the violation of privacy rights for multiple individuals. Furthermore, the geographical distribution of this issue is extensive, making it challenging to effectively address such cases through traditional offline litigation methods. For instance, if several eligible plaintiffs file lawsuits for the same case in different regions, the court would need to handle multiple cases with distinct plaintiffs but identical causes and circumstances. This type of behavior will significantly escalate unnecessary litigation costs and further strain already limited judicial resources. Hence, it is imperative to enhance both the representative litigation system and online litigation system. Currently, in China, despite the clear stipulations of the Civil Procedure Law regarding the representative litigation system, its utilization in judicial practice remains limited. The reason for this is that its provisions are abstract and they lack specific norms for the representative litigation system. Additionally, there are no clear and specific provisions for both the rights and obligations of the representative, which often leads to various problems. Therefore, improving the application of the representative system in data privacy infringement cases is of great importance.

We should work on enhancing relief measures following an event while also refining the litigation process. Currently, privacy infringement cases continue to arise within the big data environment. This stems from the fact that the cost of infringement caused by inadequate punishment is significantly low compared to the profits gained from such infringement. The profit margin associated with infringement is substantial. As a result, despite the punishment handed out to certain infringers, they persist in engaging in copyright violation. Hence, there is a need to bolster the punishment for these infringers and enhance the subsequent remedies. It is observed that if a data collection manager acquires personal information without consent, gathers citizens' private data, or employs blatantly unfair terms and clauses, and furthermore, refuses to delete it when requested, this behavior should be regarded as infringement. Severe cases should be subject to criminal sanctions.

5 Conclusion

The era of big data not only provides convenience to people's lives but also presents significant challenges to protecting data privacy. Safeguarding citizens' data privacy security and ensuring information protection is not an instant task. It requires efforts to be made in legislation, judicature, law enforcement, and compliance with the law, in line with the current circumstances. Achieving this goal necessitates cooperation across various sectors of society to collectively establish a secure and favorable online environment and alleviate the concerns surrounding data privacy.

References

[1] Hu Ling. Research on International Legal Regulation of Information Privacy in Digital Economy Era [J]. Journal of Dali University, 2022, 7 (7): 38-45.

[2] Zheng Tianyi. Research on Legal Issues of Privacy Protection in Big Data Environment [D]. Shenyang University of Technology, 2018.

[3] Pu Jinna, Bao Hu. Ethical dilemma and solution of personal privacy protection in digital age [J]. Journal of Kunming University of Science and Technology (Social Science Edition), 2023, 23 (1): 55-61. DOI: 10.16112/j.cnki.53-1160/c.2023. 01.123.

[4] Sartor, G.; Lagioia, F, The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence, Scientific Foresight Unit (STOA), European Parliamentary Research Service EPRS, 2020, p. 19 [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf], Accesed 6 July 2023.

[5] Sheng Xiaoping, Jiao Fengzhi. Data Privacy Governance from the Perspective of Domestic Laws and Regulations [J]. Library Forum, 2021, 41 (6): 85-99.

[6] Xu Mengyao. Research on Privacy Flow and Personal Information Protection in Big Data [J]. Journal of Southeast University (Philosophy and Social Sciences Edition), 2022, 24 (S1): 46-49. DOI: 10.13916/J.cnki.issn1671-511x. 2022. S1.009]

[7] Zhang Ning, Tian Li. Comparative study of personal information protection system [J]. Information Science, 2020, 38 (7): 112-116 +152. DOI: 10.13833/j.issn.1007-7634.2020.07.016.

[8] Mou Langyu. Research on Legal Protection of Personal Privacy in the Era of Big Data [D]. Chengdu: Master's Degree Thesis of Southwest Jiaotong University, 2017.

[9] Liu Ling, Luo Rong. Research on government data opening and personal privacy protection from the perspective of big data [J]. Information Science, 2017, 35 (2): 112-118.

[10] Gu Zhen. Research on Personal Information Security in Big Data Environment [J]. Information Science, 2021, 39 (12): 93-97. DOI: 10.13833/j.issn.1007-7634.2021.12.014.

[11] Zuo Weimin. Will the era of AI judges come-based on the comparison and prospect of judicial artificial intelligence between China and foreign countries [J]. Political and Legal Forum, 2021, 39 (5): 3-13.

[12] Strmecki, S., M.Sc, & Pejakovic-Dipic, S. (2023). Data Protection, Privacy And Security In The Context Of Artificial Intelligence And Conventional Methods For Law Enforcement. Osijek: J.J. Strossmayer University of Osijek. Retrieved from https://idp-lib.nenu.edu.cn/idp/shibboleth/conference-papers-proceedings/data-protection-privacy-security-context/docview/2864324916/se-2