Advances in Social Behavior Research Vol.16 Issue 4 EWA Publishing
Available Online: 10 June 2025 DOI: 10.54254/2753-7102/2025.24023

A multidimensional exploration of personal information protection in the context of social networks: case analysis and strategy discussion

Hanyu Dong[1], Xiaofang Dou[1]*

[1]School of Law, Shihezi University, Shihezi, China

*Corresponding Author. Email: 760973474@qq.com

Abstract. With the rapid development of social networks, they have become increasingly integral to people's daily lives. However, alongside the convenience brought by social networks, the issue of personal information protection has grown increasingly severe. This paper reviews domestic and international research on social networks and personal information protection, analyzes privacy and security risks as well as their underlying causes within social networks, and, through case studies, explores the balance between legal frameworks and technological solutions. It further reflects on the issue from the perspective of social ethics and highlights the necessity of international cooperation, offering corresponding policy recommendations. The aim is to reveal the current state, problems, and challenges of personal information protection in social network environments, providing both theoretical support and practical guidance to enhance personal information protection and promote the healthy, sustainable development of social networks.

Keywords: social networks, personal information protection, privacy and security

1. Introduction

According to the China Personal Information Security and Privacy Protection Report, social networks have become a major means of communication and interaction among people [1]. However, with the widespread use of social networks, the issue of personal information protection has become increasingly prominent. Social networking platforms collect, store, and process vast amounts of users' personal data. In recent years, frequent incidents of data breaches on these platforms have posed serious threats to users' privacy, property security, and even personal safety.

This paper aims to conduct a comprehensive study of social networks and personal information protection, thoroughly investigate the relevant issues, and propose effective strategies and recommendations to promote the healthy development of social networks and safeguard users' rights to personal information.

2. Literature review on social networks and personal information protection

2.1. Research status abroad

Foreign scholars began researching social networks and personal information protection relatively early and have produced a wealth of results. In theoretical studies, many researchers have explored these issues from multidisciplinary perspectives, including law and sociology.

From the legal perspective, researchers mainly focus on the legal frameworks and institutional development of personal information protection. The European Union's General Data Protection Regulation (GDPR) has been extensively studied. Scholars have analyzed the GDPR's impact on social networking platforms, including compliance costs and changes in data processing practices. The GDPR applies to data controllers or processors established outside the EU if they offer goods or services to data subjects in the EU or monitor the behavior of data subjects within the EU [2]. It has established a comprehensive system of data subject rights along with a corresponding supervisory structure. From the EU level to individual member states and down to market entities, all parties are responsible for ensuring (or at least not infringing upon) the fundamental rights related to personal data [3].

In 1997, Germany introduced the Act Regulating the Framework Conditions for Information and Communication Services. Its second part, the Telecommunications Services Data Protection Act, explicitly states that no individual or company may collect or disclose citizens' online privacy information without authorization [4]. To some extent, this legislation alleviated users' concerns about online privacy and protected citizens' "digital dignity."

In the field of sociology, research focuses on the impact of social networks on individuals' privacy perceptions and behaviors. Some empirical studies, through surveys of users' privacy behavior on social networks, found that privacy awareness varies among users and is influenced by factors such as platform design and social relationships. Users may adopt different privacy setting strategies within different social circles to balance their need for social interaction with privacy protection.

2.2. Research status in China

In recent years, research on social networks and personal information protection has been increasing in China, yielding notable achievements in both theoretical and practical dimensions.

In legal studies, following the enactment of laws and regulations such as the Cybersecurity Law and the Personal Information Protection Law, scholars have conducted in-depth analyses on the interpretation and application of relevant legal provisions. The Personal Information Protection Law of the People's Republic of China, which came into effect on November 1, 2021, is the country's first specialized and systematic legislation on personal information protection, marking a new chapter in safeguarding personal data in China [5]. Research topics include the specific meanings of legal provisions, their scope of application, and comparisons with international regulations. Some scholars have explored the compliance obligations of social networking platforms under the legal framework, such as the duty to inform and the responsibility to ensure data security.

Sociological research in China mainly focuses on how social networks influence social culture and interpersonal relationships, and the resulting issues concerning personal information protection. Some studies point out that the widespread use of social networks has altered traditional Chinese modes of interaction and perceptions of privacy. In the context of social networks, personal information spreads more rapidly and widely, making the boundaries of privacy increasingly blurred. Some users excessively share details of their personal lives on social networks, thereby increasing the risk of privacy breaches.

2.3. Commentary

Research by both domestic and international scholars in the field of social networks and personal information protection has yielded fruitful results, providing crucial theoretical support and practical guidance for the development of the field. Domestic studies have made valuable contributions by considering China's specific national conditions and the unique features of social network development. The introduction of relevant Chinese laws and regulations has offered new perspectives and foundations for academic inquiry, further advancing research in the legal domain. Overall, personal information protection in social networks is a multidisciplinary and comprehensive research field. Future research should emphasize interdisciplinary integration, align with China's practical realities, and delve deeper into the theoretical and practical issues of personal information protection in social networks, thereby promoting technological innovation and improving legal frameworks.

3. Analysis of privacy and security risks in social networks

3.1. Privacy and security risks in social networks

3.1.1. Risk of personal information leakage

Social networking platforms collect vast amounts of users' personal information, and there are risks of information leakage during storage, transmission, and processing. On one hand, security vulnerabilities within the platforms themselves may lead to data breaches. Hackers can exploit software loopholes, weak passwords, and other issues to infiltrate platform servers and obtain users' personal data. On the other hand, data sharing between social networking platforms and third-party partners also heightens the risk of data leakage. If third-party partners lack adequate security measures or violate data usage agreements, users' personal information may be exposed.

The "privacy paradox" is widespread—many internet users lack basic awareness of personal information protection and show little concern about the privacy safeguards implemented by social networking sites, which undoubtedly increases the risk of privacy breaches [6].

3.1.2. Risk of privacy infringement

Users' actions and expressions on social networks may result in privacy infringements. Photos, location data, and personal details shared by users can be exploited by others to violate their privacy. Some individuals analyze others' social media content to obtain sensitive information such as travel patterns or home addresses, leading to stalking or harassment. Moreover, the phenomenon of

"human flesh search" (online crowdsourced doxxing) on social networks seriously invades individuals' privacy. The problem of privacy breaches hidden behind the popularity of social networks is becoming increasingly severe. Over 30% of surveyed individuals or organizations have experienced security incidents, such as receiving spam, unauthorized use of personal information, or compromised accounts with altered passwords [7].

3.1.3. Risk of identity theft

Identity theft refers specifically to fraudulent behavior involving impersonation on the internet. Criminals may pose as celebrities, entrepreneurs, or government officials to gain others' trust for personal gain, or they may steal the personal data of ordinary individuals to attack specific people or organizations [8].

Personal information leaks on social networks may lead to identity theft. Once criminals obtain users' personal data, they can use it to create false identities and engage in illegal activities such as fraud or unauthorized loans. Hackers who acquire users' bank card details and identification numbers may forge bank cards and conduct fraudulent transactions or apply for online loans using stolen identities, resulting in financial losses and credit risks for the victims.

3.2. Analysis of the causes of privacy infringement on social networks

3.2.1. Technical vulnerabilities and security risks

One of the primary causes of privacy infringement on social networks is the presence of loopholes in the platform's technical architecture and security measures. On the one hand, software development may involve defects in code and improper security configurations, rendering the platform susceptible to hacker attacks. Moreover, artificial intelligence algorithms, while analyzing user data, may inadvertently expose users' sensitive information. In addition, existing legal regulations are insufficient to address data breaches and illegal use triggered by digital technologies, thereby exacerbating the consequences of privacy infringements [9]. Delays in implementing or inadequately enforcing certain security measures leave many potential threats unresolved in time, posing ongoing and serious challenges to the overall security of network systems [10].

3.2.2. Inadequate platform management

Social networking platforms often exhibit deficiencies in managing user information. During the data collection process, platforms may collect excessive user information that exceeds the scope necessary for service provision. Some social applications, during user registration, request an overabundance of personal details such as occupation, income, and marital status—information that is unrelated to the core functionality of the application. Relevant personnel must possess strong information ethics and professional competence, reinforce awareness of personal information protection, and enhance the construction and management of information security systems.

3.2.3. Users' lack of security awareness

A lack of awareness among users about security and privacy protection is also a significant factor contributing to privacy violations. Many users fail to prioritize safeguarding their personal information when using social networks and share sensitive data recklessly. For example, users may disclose their ID numbers, bank card details, or access their accounts via unsecured public networks without taking precautions to protect passwords. Additionally, users often overlook privacy policies and terms of service, remaining unaware of how their information is collected, used, and protected. As a result, they consent to privacy agreements without fully considering the potential risks involved.

4. Case analysis

4.1. Case study: Qi's infringement of citizens' personal information

Between September and October 2021, Qi, taking advantage of access to vehicle information, conducted 61 vehicle information inquiries on behalf of Ji, gaining an illegal profit of 1,525 yuan. The two deleted the related data afterward. However, investigations revealed that the information Ji obtained was publicly accessible and could be retrieved through self-service terminals at the vehicle administration office or third-party platforms. Separately, Qi sold traffic accident-related information acquired through his job to Wen Moujiaguang and even added him to the Nan'gang Traffic Police Incident Response Group. Wen Moujiaguang used this information to contact the parties involved in traffic accidents and profit from repair arrangements. Upon verification, Qi had illegally provided a total of 1,514 entries of citizens' personal information—such as accident time, location, vehicle model, and license plate number—earning 29,160 yuan unlawfully. During the second trial, Qi's relatives returned the illicit gains of 29,160 yuan and paid the corresponding fine on his behalf.

According to Articles 253-1, Paragraphs 1 and 2 of the Criminal Law of the People's Republic of China, Qi's actions—violating national regulations by selling citizens' personal information obtained during his duties as an auxiliary police officer—constituted the crime of infringing upon citizens' personal information. Per Article 1 of the Interpretation on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving Infringement of Citizens' Personal Information, "citizens' personal information" refers to various types of information recorded in electronic or other forms that can identify a specific natural person individually or in combination with other data, or reflect their activities. In this case, the incident information Qi sold was closely tied to specific individuals involved in the accidents. The data was targeted, non-public, and, if disclosed, could harm the involved parties' personal rights, thus meeting the criteria for "citizens' personal information" as defined in the statute. The second-instance court upheld the conviction in the first-instance criminal judgment No. 164 (2024) by the Nan'gang District People's Court of Harbin, Heilongjiang Province, confirming that Qi was guilty of infringing on citizens' personal information.

Citizens' personal information includes all data that can identify a specific individual or reflect their activities, and it is closely related to the personal safety, financial security, and privacy of individuals. In this case, the traffic accident information sold by Qi—containing accident times, locations, vehicle models, and license plate numbers—posed risks of fraud, harassment, and other harms once leaked. This case fully illustrates the critical importance of personal information protection in safeguarding citizens' fundamental rights and interests.

4.2. The balance between law and technology

4.2.1. Coordinated development of technological innovation and privacy protection

Technological innovation plays a crucial role in protecting personal information on social networking platforms. On one hand, emerging technologies such as encryption, blockchain, and differential privacy can enhance the security of personal data. On the other hand, the need for privacy protection can also drive technological advancements. As users' demands for privacy continue to grow, social networking platforms and technology developers are compelled to explore new technical solutions to meet these expectations. In an effort to safeguard user privacy, some platforms have begun adopting anonymization techniques to process personal data, enabling data analysis and application without compromising users' private information.

4.2.2. Strategies for protecting personal information rights on social networks

First, from a technological perspective, social networking platforms should increase investment in security technologies and adopt advanced measures to protect users' personal data. This includes the use of multi-factor authentication to prevent account hijacking and the establishment of strict access control mechanisms to ensure that only authorized personnel can access sensitive information based on users' roles and permissions. Moreover, platforms should implement anonymization and de-identification techniques during data analysis and application, removing identifiable personal information and retaining only statistical data. This approach allows platforms to fulfill their data and business needs while safeguarding user privacy.

Second, in terms of user privacy awareness, as the primary subjects of personal data, users' awareness and behaviors are vital to privacy protection. However, many users currently exhibit a relatively weak understanding of data protection in the context of social networks. On one hand, they may underestimate the importance of personal data and casually share sensitive information online. On the other hand, when confronted with privacy policies and service agreements, users often lack the patience and expertise to comprehend the complex content, resulting in uninformed consent to the platform's data collection and usage terms.

Furthermore, social networking platforms have a responsibility to educate and guide users in protecting their personal information. Platforms should enhance security prompts and remind users to be mindful of privacy protection. During registration, login, or information sharing, platforms can issue alerts advising users on best practices, such as setting strong passwords and avoiding suspicious links. Additionally, platforms can offer practical privacy protection tools and features, such as privacy setting wizards to help users configure permissions according to their needs, and account security check functions to identify vulnerabilities and provide appropriate solutions.

5. International cooperation and policy recommendations

5.1. The necessity of international cooperation in personal information protection

In the context of globalization, users and data on social networking platforms transcend national borders, presenting numerous challenges to the protection of personal information. As such, international cooperation is of critical importance in addressing these challenges. The cross-border flow of personal information affects both national and international governance, and there remains a need within the international community to adjust and regulate such activities [11].

First, international cooperation facilitates the sharing of information and exchange of experiences among different countries and regions. Given the diversity in legal frameworks, policies, and practical approaches to personal information protection,

international collaboration allows countries to learn from one another, adopt successful practices, and collectively enhance their capabilities in protecting personal information.

Second, international cooperation strengthens the regulation of transnational social networking platforms. The operations of these platforms often span multiple countries and regions, making it difficult for any single nation to effectively oversee their activities. Through cooperative mechanisms, countries can establish joint regulatory frameworks to ensure that these platforms comply with the personal information protection laws of all jurisdictions involved, thereby preventing regulatory evasion due to legal disparities across regions.

5.2. Policy recommendations for strengthening international cooperation

Countries should enhance communication and coordination by establishing dedicated international cooperation mechanisms responsible for managing cross-border collaboration on personal information protection. These mechanisms could convene regular meetings to discuss emerging issues, formulate cooperative strategies, and implement joint measures. An information-sharing platform could also be created to promote the exchange and dissemination of data protection knowledge across countries. Furthermore, international organizations and individual countries can work together to develop unified global standards for personal information protection. These standards should encompass all aspects of data handling—including collection, usage, storage, and sharing—and clearly define the rights and responsibilities of all parties. Unified standards would provide clear operational guidance for transnational social networking platforms and facilitate cross-border regulatory cooperation.

On the technological front, countries can deepen collaboration in the development and deployment of personal information protection technologies. This includes the joint research and promotion of advanced technical solutions, as well as further investigation into emerging technologies such as artificial intelligence and blockchain, to explore their potential in enhancing data privacy. In terms of educational cooperation, global awareness of personal information protection should be improved through international campaigns and educational initiatives. Countries can conduct joint awareness efforts to disseminate knowledge and practical skills related to data protection, thereby strengthening the public's ability to safeguard their personal information. Simultaneously, education targeted at social networking platforms and enterprises should be intensified, encouraging compliance with relevant laws, regulations, and international standards for personal information protection.

6. Conclusion

This study has certain limitations. From a technical perspective, although several data protection technologies were discussed, the rapid pace of technological advancement means that not all the latest methods and applications could be covered. In summary, the intersection of social networking and personal information protection represents a research area of significant theoretical and practical relevance. Ongoing in-depth investigation is essential to meet the evolving demands of rapidly developing social networks and to effectively safeguard users' personal information rights.

References

[1] Yang, R., Li, H., & Sun, Z. (2024). Privacy protection of social network data: Origin, technology, policy, and prospects. *Journal of Agricultural Library and Information Science, 36*(4), 4–20.
[2] Zheng, Z. (2022). A brief analysis of the EU General Data Protection Regulation and its compliance requirements. *China COSCO Shipping*, (4), 48–52.
[3] Tian, Y. (2025). Personal information protection in government data openness: EU experience and enlightenment—Reflections based on the EU General Data Protection Regulation. *Journal of Yibin University*, 1–8. Advance online publication.
[4] Zhao, P., & Mou, Y. (2016). Research on privacy and security issues based on social media platforms. *Journal of Chengdu Administrative College*, (6), 26–28.
[5] Wang, X., & Li, Y. (2023). Legislative value, jurisprudential dimension, and legal philosophy of the Personal Information Protection Law. *Information and Documentation Services, 44*(3), 42–48.
[6] He, J., Luo, Y., & Teng, L. (2017). Privacy security issues of social network users and their protection. *Network Security Technology and Application,* (11), 149–150.
[7] Xiao, H., & Zhu, X. (2018). Research on social network security issues and countermeasures based on big data. *Information System Engineering*, (2), 79–81.
[8] Zhu, X., Jiang, D., & Yang, C. (2015). Analysis and discussion on security risks of social networks. *Telecommunication Technology, 48*(2), 219–222.
[9] Qi, X., Zhang, Y., & Feng, E. (2017). Research on privacy protection issues of mobile social network users. *Forum on Industry and Technology, 16*(16), 35–36.
[10] Zeng, X. (2024). Information security and privacy protection technology in communication networks. *Software, 45*(8), 108–110.
[11] Yao, R. (2024). International soft law governance of cross-border personal information protection and China's approach. *Wuhan University International Law Review, 8*(4), 56–75.