

Network privacy protection and legal system in the digital era

Meiqi Qi¹, Xichang Yao², Qianqian Zhu³, Ge Jin^{4,*}

¹*School of Marxism, Shaanxi Normal University, Xi'an, Shaanxi, China*

²*School of Marxism, Yellow River Institute of Communications, Zhengzhou, Henan, China*

³*School of Marxism, Henan Police College, Zhengzhou, Henan, China*

⁴*Law School, Hainan University, Haikou, Hainan, China*

**Corresponding author*

Keywords: Digital age; network privacy protection; legal system

Abstract: In the digital age, the rapid development of the Internet has brought great convenience to people's lives, but it has also caused a series of network privacy protection problems. The leakage and abuse of personal information on the Internet has become a common phenomenon, which has brought a serious impact on people's life and work. Therefore, it is of great practical significance to discuss the network privacy protection and legal system in the digital era. This paper discusses the importance of network privacy protection and legal system in the digital era. With the popularity of the Internet, the spread of personal information on the Internet is more and more extensive, but the problem of network privacy also follows. The existing legal system is insufficient in the protection of network privacy, and it needs to be further improved. By comparing the legal system of network privacy protection in different countries and regions, this paper puts forward some suggestions to improve the legal system of network privacy protection in China.

1. Introduction

The importance of network privacy protection and legal system is becoming more and more important in the digital age. Online privacy issues not only involve the security and protection of personal information, but also are related to national security, social stability and public order. Through the establishment of a strong legal system, the behavior of network operators and Internet enterprises can be regulated, and the security risks such as network attacks and data leakage can be prevented, so as to maintain the stability and security of the network. In addition, strengthening the construction of the legal system for online privacy protection also helps to promote the development of the digital economy, protect the security of personal information, enhance individuals' trust in the digital economy, and promote the healthy development of the digital economy. At the same time, the occurrence of network privacy problems may also lead to social instability and the destruction of public order, and through the establishment of a sound legal system, the supervision and punishment can be strengthened to prevent the occurrence of network privacy infringement, and maintain social stability and public order[1]. To sum up, strengthening the construction of the legal system of network privacy protection is crucial to meet the needs of network privacy protection in

the digital era.

2. The importance of online privacy protection

2.1. The definition and importance of privacy rights

Privacy right is the core concept of personal information protection, which has important legal significance and social value. In the digital age, network privacy protection is particularly important, because the dissemination and use of personal information in the network has become more widespread and universal. The right of privacy refers to the right to protect his personal information, that is, the right of the individual's right to determine the acquisition and dissemination of his personal information by others[2]. The importance of privacy rights is reflected in the following aspects: First, the right to privacy is the embodiment of personal dignity and personality rights, and everyone has the right to protect their own personal life and privacy. Secondly, the right to privacy is the basis of information security and network security, and the development and application of cyberspace needs a good privacy protection mechanism to protect personal and social security. Thirdly, the right to privacy plays an important role in promoting personal freedom, innovation and development. Individuals need to have a privacy protection environment to express themselves and explore various new possibilities. In addition, privacy is essential to building trust and maintaining fair competition. Only with privacy protection will individuals be willing to share their information to promote the prosperity of the digital economy and society. In short, the importance of network privacy protection can not be ignored. It is necessary to establish sound laws and systems to protect individual privacy rights and interests to promote the sustainable development of the digital age.

2.2. Privacy protection challenges in the digital age

The challenge of privacy protection in the digital era refers to that in the digital era, with the rapid development of the Internet and information technology, personal privacy is facing unprecedented challenges and threats. First, as people move more frequently on the Internet, personal information is becoming more and more easy to obtain and use. For example, the photos, personal data, geographical location and other information posted by individuals on social media may be used by criminals to carry out illegal activities such as identity theft and fraud. Secondly, the wide application of big data and artificial intelligence technology enables personal privacy to be more accurately collected and analyzed. By analyzing individuals' network browsing records, shopping habits, social relations and other information, enterprises and governments can obtain a large amount of sensitive information about individuals, which may violate individuals' privacy rights[3]. In addition, the global nature of the Internet and the cross-border mobility of information make personal privacy face the challenges of transnational monitoring and cross-border data flow. Governments or organizations may use technology to monitor and track individuals, which not only infringes on their privacy rights, but also poses a threat to the stability and security of the international community. Therefore, the privacy protection in the digital age is faced with many challenges, and it is necessary to establish an effective legal system and technical means to strengthen the protection of personal privacy.

2.3. The potential risk of privacy leakage

The potential risk of privacy leakage refers to the risk and harm that personal privacy may be leaked or violated in the digital age[4]. With the development and popularization of network technology, personal privacy information is more and more easy to be obtained and used by others.

Once personal privacy information is leaked, it may lead to a variety of adverse consequences, including but not limited to the following aspects.

First, privacy leakage may lead to the abuse of personal information. Once the personal information falls into the hands of the criminals, they can use the information for a variety of illegal activities, such as stealing personal property and committing online fraud. In addition, some criminals will also buy and sell personal information, further aggravating the abuse of personal information.

Second, privacy leakage may bring personal social and psychological distress[5]. With the disclosure of personal information, personal habits, interests and hobbies are understood by others, which may lead to individuals feel the freedom of loss and security of privacy. For some special groups, such as public figures and celebrities, it is more likely to become the focus of media and public attention, and such attention often brings inconvenience in life and psychological pressure to individuals.

In addition, privacy leakage may also have a negative impact on the professional and personal image. In the digital age, personal social network activities and personal images are increasingly associated with professional images[6]. Once the personal privacy information is leaked, it may be caught by others, maliciously distort the personal occupation and image, and bring adverse effects on the personal career development and personal reputation.

Finally, privacy disclosure may also cause physical and mental health problems to individuals. In the digital age, people's private information can be obtained through various means, which may lead to a sense of individuals being monitored and tracked, thus having a negative impact on their physical and mental health, such as anxiety and depression.

3. The shortcomings of the current legal system of network privacy protection

3.1. The legal framework of privacy protection is incomplete

The incomplete legal framework of the current network privacy protection is mainly reflected in the following aspects. First of all, with the development of the digital age, the traditional legal framework of privacy protection has been unable to meet the needs of network privacy protection under the new situation. The current legal system often only involves the protection of personal information, and lacks clear regulations for other forms of network privacy, such as network behavior data. Secondly, the current legal framework has vague problems in the scope of privacy protection, the definition of rights and obligations, and the responsibility mechanism. Privacy protection laws often lack specific and clear provisions, which makes it difficult to implement the protection of privacy rights in practice. In addition, the current law is not strict enough on the collection, use and transmission of personal information, and lacks effective measures to ensure the security of personal information[7]. Also important, compared with the development speed of technology, the current legal framework is slower, unable to keep up with the pace of The Times, resulting in the legal system appears powerless to cope with the emerging privacy protection issues. Therefore, the current legal system of network privacy protection is insufficient, which needs to be strengthened and improved.

3.2. The difficulty of enforcing the privacy protection law

The shortcomings of the current network privacy protection legal system are mainly reflected in the difficulties in the implementation of the privacy protection law. First of all, there is a lack of uniform norms in the implementation of privacy protection laws. Due to the cross-border and diversification of network privacy in the digital era, there are differences in the legal systems of

privacy protection in different countries and regions, and the lack of unified international standards and norms. This makes it difficult to achieve effective privacy protection in cross-border cooperation and cross-border data transmission. Second, privacy protection laws face technical challenges in the implementation process. With the continuous progress of technology, the means of privacy invasion are also constantly updated, and the traditional legal means are difficult to conform to the pace of technology development, leading to the lag of law enforcement. At the same time, there are also difficulties in implementing the privacy protection law in its practical application. On the one hand, the specific provisions of privacy protection laws are difficult to implement and operate, and lack of operability[8]. On the other hand, the enforcement agencies and law enforcement personnel of privacy protection laws are insufficient in technical expertise and law enforcement ability, resulting in poor enforcement effect. To sum up, the shortcomings of the current network privacy protection legal system mainly focus on the difficulties in the implementation of the privacy protection law.

3.3. The gap between privacy protection laws and technology

The gap between privacy protection law and technology refers to the shortcomings of the current network privacy protection legal system in the face of the rapidly developing technological change in the current digital era. With the rapid development of science and technology, the gap between the network privacy protection law and technology is increasing. First, technological innovations and advances have made it easier to collect and use personal data and difficult to regulate and control. The legal provisions of personal data protection do not match the speed of technology development, and they cannot adapt to the application and change of new technologies in time. Secondly, the current legal system of privacy protection generally has institutional loopholes and insufficient supervision. For the emerging network privacy infringement, the law does not clearly stipulate, resulting in the legal gap of privacy protection. In addition, the legal system has problems in the implementation and supervision of privacy protection measures, and the supervision is insufficient and the implementation is not good effect. Thirdly, the complexity and diversity of technology make there is a gap between the technical means of privacy protection and the legal provisions. The update and application of privacy protection technology is much faster than the formulation and improvement of laws, and the adaptation and specification of laws to new technologies lag behind the development of technology. Therefore, the shortcomings of the current network privacy protection legal system are mainly reflected in the gap between the privacy protection law and technology.

4. Construction of a legal system for network privacy protection in the digital era

4.1. Strengthen the improvement of the legal framework for privacy protection

With the advent of the digital era, the problem of network privacy protection is becoming increasingly prominent, and it is urgent to establish a perfect legal system to protect personal privacy rights. In this context, it has become a very important task to improve the legal framework of privacy protection.

First, a sound legal framework for privacy protection is needed. At present, the legal provisions related to privacy protection are relatively lagging behind, and they cannot well adapt to the complexity and diversity of network privacy issues in the digital era[9]. Therefore, the legal framework of privacy protection should be improved by formulating new laws and regulations or revising existing laws. These laws should clearly stipulate the principles and norms to be followed in the collection, use, storage and transmission of personal information, and clearly stipulate the

legal responsibility for acts that violate privacy protection.

Secondly, a sound supervision mechanism should be established. The effective implementation of privacy protection needs the supervision and management of relevant regulatory agencies or departments. These institutions shall be responsible for supervising whether network service providers, data processors and other relevant subjects fulfill their responsibilities for privacy protection according to law, investigate and punish illegal acts, and provide timely and effective relief measures.

In addition, technical means to strengthen privacy protection. With the rapid development of science and technology, the leakage and abuse of personal information are also increasingly diverse and hidden. Therefore, the ability of network privacy protection should be enhanced by strengthening the research and development and application of technical means. For example, encryption technology, decentralized storage technology and other means can be used to ensure the security and privacy of personal information in the process of transmission and storage.

Finally, the relief mechanism of privacy protection should be improved. When individual privacy rights and interests are infringed, an effective relief mechanism is needed to protect their legitimate rights and interests. Therefore, the tort compensation system should be established and improved, making it clear that individuals can obtain corresponding compensation through legal channels. At the same time, social forces should be encouraged to participate in privacy protection and safeguard their legitimate rights and interests by means of prosecution and complaint.

4.2. Explore the combination path of privacy protection law and technology

One of the keys to the construction of network privacy protection legal system in the digital era is to explore the combination path of privacy protection law and technology. In the process of building the legal system of network privacy protection, the traditional legal means are not perfect and efficient. Therefore, combining with technical means has become a necessary way to improve the effect of network privacy protection. First, the supervision and guidance of technology development need to be strengthened to ensure that the application of technology meets the requirements of privacy protection laws. In the digital age, with the rapid development of technology, many new technologies have emerged that may violate personal privacy. Therefore, through the establishment of technical norms and standards compatible with the privacy protection laws, the research and development, application and supervision of new technologies should be comprehensively managed, so as to ensure the security of personal privacy[10].

Secondly, we need to actively promote the cooperation and collaboration between law and technology. Traditional legal means may have some limitations in dealing with the network privacy protection problem, which cannot fully meet the actual needs. Therefore, combining law and technology and assisting the implementation of legal means through technical means can improve the effect of network privacy protection. For example, through the use of encryption technology, anonymity technology and authority management technology, strengthen the protection of personal privacy information, and formulate corresponding regulations and measures at the legal level.

In addition, it is necessary to increase the support for technology research and development and innovation to promote the continuous upgrading of technology and law. In the digital era, network privacy protection is facing new challenges and threats, so it is necessary to continuously promote the innovation and development of technology to adapt to the needs of privacy protection under the new situation. By encouraging science and technology enterprises and research institutions to increase investment in the research and development of privacy protection technologies, promote the continuous upgrading and improvement of technology and law, and maintain the synchronization and efficiency of legal system and technical means.

5. Conclusions

The importance of strengthening the construction of the legal system of network privacy protection is reflected in the following aspects: First, the right of privacy is the embodiment of personal dignity and personality rights, and the protection of personal privacy is the right of everyone. Secondly, network privacy protection is the basis of information security and network security, and a good privacy protection mechanism is needed to protect personal and social security. Thirdly, network privacy protection plays an important role in individual freedom, innovation and development, and it is necessary to create an environment with privacy protection. In addition, online privacy protection is also crucial to building trust and maintaining fair competition. Only under the premise of privacy protection, individuals will be willing to share their information and promote the development of digital economy and society. Therefore, it is very necessary to strengthen the construction of the network privacy protection legal system. At the same time, it is also important to promote international cooperation and sharing experience, because the network privacy protection issue has global characteristics, which needs to cooperate across national boundaries to jointly meet challenges, form global network privacy protection standards and norms, and improve the level of network privacy protection through sharing experience.

Acknowledgements

Major subject of educational science planning in Henan Province: Research on the dilemma and countermeasures of basic education Group in running a school under the background of "double reduction" (2024JKZD50).

References

- [1] Zhang Ke. *Research on Computer Network Information Security and Its Protection Countermeasures* [J]. *Office Automation*, 2023, 28 (14): 19-21.
- [2] Wang Wei, He Xin, Chen Kunhua, et al. *Traceability and countermeasure technology for common information security attack tools* [J]. *Network Security Technology and Application*, 2023 (07): 8-9.
- [3] Song Lei. *Information Security Problems and Its Countermeasures in modern Information Technology Environment* [J]. *Science and Technology Wind*, 2023 (16): 69-71.
- [4] Zhang Juanping, Zhang Hailiang. *Big data and data privacy protection related issues research* [J]. *Software*. 2023.44(02):81-84.
- [5] Bian Na. *Research on typical risk and Guarantee Mechanism of Big Data Information Security* [J]. *Volkswagen Standardization*, 2022 (19): 110-112.
- [6] Gu Yun. *Discussion on information security, network security and privacy protection* [J]. *Digital Communication World*, 2021 (07): 150-151 + 86
- [7] Wang Jiang, Fan Xiangdong, Shi Wei. *Research on Network Information Security and Privacy Protection in the Era of Big Data* [J]. *Information and Computer (theoretical edition)*, 2018 (24): 213-214 + 217
- [8] Liu Mingzheng, Sun Dongxin. *Impact of Internet literacy on user privacy concerns and privacy protection self-efficacy* [J]. *Journal of Shenyang University (Social Science Edition)*, 2023, 25 (01): 47-54 + 78.
- [9] Wang Xiaoting, Wang Qingsheng, Chen Yongle. *GAN based on social networks* [J]. *Computer Engineering and Design*, 2023, 44 (04): 991-997.
- [10] Yang Xintao, Li Yunpeng, Chang Jinming. *Research on information security, network security and privacy protection* [J]. *Information System Engineering*, 2023, (09): 138-141.