Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 7, No. 3, 2024
www.scholink.org/ojs/index.php/elp

Original Paper

Criminal Regulation of Illegal Use of Citizens' Personal Information

Yanqiu Xiong[1*] & Minna Qiu[2]

[1] The discipline inspection and supervision group of the Anqing City Discipline Inspection Commission in the Anqing Municipal People's Congress, Anqing, China

[2] Law School, Shantou University, Guangzhou, China

Received: October 25, 2024 Accepted: November 8, 2024 Online Published: November 13, 2024

doi:10.22158/elp.v7n3p96 URL: http://dx.doi.org/10.22158/elp.v7n3p96

Abstract

With the rapid development of information technology, the collection, storage, and use of citizens' personal information have become increasingly convenient. At the same time, the illegal use of personal information has become rampant, seriously threatening personal privacy rights and social order. This paper aims to systematically explore the criminal regulation of illegal use of citizens' personal information. It first defines the concept and classification of personal information, then analyzes the specific forms of illegal use of personal information. Through a comparative study of relevant laws and regulations domestically and internationally, it reveals the effectiveness and deficiencies of current criminal regulations in protecting personal information. The research finds that although China has made progress in personal information protection legislation, there are still significant shortcomings in defining criminal liability, clarifying the application of laws, and enforcing regulations. Based on this, the paper proposes several recommendations to improve criminal regulation, including clarifying the constitutive elements of crimes, strengthening law enforcement, enhancing public awareness, and promoting international cooperation, with the aim of providing theoretical support and practical guidance for further improving China's legal system for personal information protection.

Keywords

Illegal use, citizens' personal information, criminal regulation, legal liability

1. Introduction

In the context of the information age, the collection, storage, and utilization of personal information have become an integral part of societal operations. With the rapid development of the internet, big data, and artificial intelligence technologies, the acquisition of citizens' personal information has become unprecedentedly convenient. However, the rapid progress of information technology has also posed severe challenges, as the illegal use of citizens' personal information has become rampant, seriously infringing upon personal privacy, undermining social trust, and even threatening national security and social stability. In recent years, various cases of personal information leaks and misuse have frequently occurred, significantly raising public awareness of personal information protection. Against this backdrop, effectively curbing the illegal use of personal information has become an urgent legal issue. Criminal regulation, as an essential means for the state to combat crime and maintain social order, plays an increasingly prominent role in protecting personal information. However, the current criminal law still faces numerous inadequacies in addressing new types of information crimes, necessitating further refinement and strengthening. This study aims to systematically explore the criminal regulation of illegal use of citizens' personal information by reviewing and analyzing relevant laws and regulations, revealing the application of existing criminal laws in personal information protection and their deficiencies (Zhang & Dong, 2023, p. 64). The specific objectives include defining the legal concept and classification of personal information, clarifying the specific forms of illegal use of personal information, conducting a comparative analysis of domestic and international legal provisions on personal information protection to draw on advanced experiences, and proposing feasible recommendations to address the shortcomings of current criminal regulation. The significance of this research lies in providing theoretical support for improving China's legal system for personal information protection, promoting scientific and systematic legislation, and offering references for law enforcement practices to enhance the effectiveness of combating the illegal use of personal information and ultimately safeguarding citizens' legitimate rights and interests, as well as maintaining social justice and fairness. This research primarily adopts a combination of literature analysis, comparative study, and case analysis methods. First, it systematically reviews domestic and international laws and regulations on personal information protection and relevant academic studies to construct the theoretical framework for this research. Next, it selects representative countries and regions, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in the United States, for comparative analysis, drawing on their advanced experiences and practices in criminal regulation. Subsequently, it examines several typical cases to analyze the determination of criminal liability and the practical issues in applying the law to the illegal use of personal information. Finally, based on the research findings, it proposes specific recommendations to improve China's criminal regulation of the illegal use of personal information. Through these methods, the study seeks to comprehensively and systematically explore the criminal regulation of illegal use of citizens' personal information, providing valuable references for relevant legislation and law

enforcement practices (Chang, 2023, pp. 19-26).

2. Conceptual Definitions and Theoretical Basis

Before discussing the criminal regulation of illegal use of citizens' personal information, it is necessary to clearly define relevant concepts and construct the theoretical basis for the research. This chapter first defines personal information and its classification, then clarifies the specific forms of illegal use of personal information, and finally explores the theoretical basis for criminal regulation to provide a solid foundation for subsequent legal analysis (Petrović, 2022, pp. 469-489).

2.1 Definition and Classification of Personal Information

Personal information refers to various information recorded by electronic or other means that can identify a natural person either individually or in combination with other information. According to the Personal Information Protection Law of the People's Republic of China, personal information includes but is not limited to names, dates of birth, identification numbers, personal biometric information, addresses, phone numbers, and email addresses (Petrović, 2022, pp. 469-489). Protecting personal information is crucial for safeguarding citizens' privacy rights and personal dignity. Personal information can be categorized based on its sensitivity and potential impact on personal rights. Generally, personal information is divided into two categories: sensitive information and non-sensitive information. Sensitive information refers to information that, if leaked or misused, may severely harm a person's privacy, reputation, or financial interests, such as biometric data, religious beliefs, genetic information, medical and health data, and financial account information (Giannakoula, Dafni & Maria, 2020, pp. 1-97). Due to its high sensitivity, the collection, storage, and use of sensitive information are subject to stricter legal restrictions and protections. Non-sensitive information refers to basic information that relatively does not involve core personal privacy, such as names, ages, genders, addresses, and phone numbers. Although the protection requirements for non-sensitive information are relatively relaxed, its legitimate use and misuse prevention remain crucial aspects of information protection, especially in the age of big data, where the combination of such data with other information can still pose privacy risks. Therefore, safeguarding the legitimate use and preventing the misuse of even non-sensitive information is an important part of comprehensive information protection (Tong, 2023, p. 110).

2.2 Defining Illegal Use of Personal Information

The illegal use of personal information primarily includes unauthorized acquisition, illegal sale, illegal dissemination, and other related unlawful activities. These behaviors not only infringe upon individual privacy but can also lead to financial loss, identity theft, and even pose threats to public security. Unauthorized acquisition refers to the unauthorized collection, acquisition, purchase, use, processing, transmission, provision, or public disclosure of others' personal information beyond the scope of legitimate authorization (Oliinyk et al., 2020, pp. 445-459). Methods for illegally obtaining personal information are diverse, including network attacks, phishing scams, and insider leaks. Illegal sale

involves selling acquired personal information in any form for profit. This behavior infringes on the rights of information subjects and promotes the illegal trade of personal information, further exacerbating the problem of information misuse. Illegal dissemination is the unauthorized disclosure, dissemination, public sharing, or posting of others' personal information on online platforms. This not only broadens the scope of information leakage but can also trigger larger-scale privacy violations and social panic. Other related behaviors include using personal information for fraud, extortion, harassment, and identity theft, which often have high degrees of concealment and complexity, posing significant challenges to regulatory and enforcement efforts (Oliinyk et al., 2020, pp. 445-459).

2.3 Theoretical Basis for Criminal Regulation

Criminal regulation of the illegal use of personal information relies on a range of legal theories that guide legislation and enforcement. The legal protection theory emphasizes that the core function of the law is to protect public interests and individual legal rights. Personal information, as an important social resource, relates not only to individual privacy and dignity but also to social trust and public security. Therefore, criminal regulation reflects the law's firm commitment to safeguarding the rights and interests of information subjects (Zhao, 2023, p. 674). The crime prevention theory focuses on preventing crimes through legal means. By imposing criminal penalties for the illegal use of personal information, the law serves as a deterrent, reducing potential offenders' motivations and behaviors. Stringent criminal regulations also promote the lawful use of information and contribute to healthy social information order. The accountability theory highlights the identification and accountability of unlawful behavior. Criminal regulation not only punishes illegal acts but also holds perpetrators accountable, reinforcing the authority and fairness of the law, and enhancing public trust and confidence in legal enforcement. In summary, defining personal information and its classification, clarifying the specific forms of illegal use of personal information, and constructing the theoretical basis for criminal regulation are essential for in-depth research on criminal regulation. These theories and clearly defined concepts provide a solid foundation for subsequent legal analyses and policy recommendations (Zhu & Song, 2022).

3. Domestic and International Legal Provisions on the Illegal Use of Personal Information

With the rapid development of information technology, personal information protection has become a global focal point. Internationally, the European Union enacted the General Data Protection Regulation (GDPR) in 2018, which is currently the most comprehensive and stringent data protection law. The GDPR grants broad rights to data subjects, such as the right to be informed, the right to access, and the right to erasure, while imposing strict compliance requirements on data processors. Violations may result in hefty fines of up to 4% of the global annual turnover or 20 million euros, whichever is higher. Additionally, in 2020, California implemented the California Consumer Privacy Act (CCPA), which provides consumers with more control over their personal information and regulates corporate data processing practices, with significant penalties for noncompliance. In comparison, China has also made

significant progress in personal information protection. The enactment of the Personal Information Protection Law (PIPL) in 2021 systematically regulates the collection, storage, use, and transfer of personal information, clarifies the rights of data subjects and the obligations of data processors, and establishes strict legal liabilities, including administrative and criminal responsibilities. The introduction of PIPL marks China's entry into a new stage of legalized and standardized personal information protection (Pang, 2021, pp. 1-12). Nevertheless, compared with advanced regulations like the GDPR, China still has room for improvement in implementing mechanisms for data subject rights, regulating cross-border data transfers, and refining criminal responsibilities. Comparative analysis reveals that international regulations have higher standards for data protection systems and enforcement, while China's legal framework is gradually closing the gap. In the future, China can draw on the successful experience of the GDPR to further refine legal provisions, enhance enforceability, and ensure the effective implementation of personal information protection laws, thereby playing a more significant role in global data governance.

4. Analysis of Criminal Liability for the Illegal Use of Personal Information

The illegal use of personal information not only infringes upon individual privacy rights but also poses a threat to public security and economic order. Analyzing the criminal liability of such behavior helps clarify legal boundaries, strengthen legal deterrence, and protect citizens' legitimate rights. This chapter analyzes criminal liability from three aspects: the constitutive elements of criminal liability, existing legal provisions and their application, and the issues and challenges in law enforcement. First, the constitutive elements of criminal liability include subject elements, object elements, subjective elements, and act elements. Subject elements require that the criminal act be committed by a natural person with criminal responsibility capacity, meaning the person must have full civil capacity and corresponding criminal responsibility capacity (Shanshan & Tao, 2022, pp. 64-71). Object elements involve the legal interest protected by law, primarily focusing on individual privacy and information security in cases of illegal use of personal information. Subjective elements include intent and negligence, with most illegal uses of personal information being intentional acts where the perpetrator knowingly violates others' rights. Act elements refer to the specific acts of the offender, such as unauthorized acquisition, sale, or dissemination of others' personal information. Second, current legal provisions on the illegal use of personal information are primarily reflected in the Criminal Law of the People's Republic of China and the Personal Information Protection Law. Article 253 of the Criminal Law specifies the crime of infringing on citizens' personal information, criminalizing the unauthorized acquisition, sale, or provision of personal information, with a maximum penalty of three years' imprisonment or detention, and fines. In severe cases, such as acquiring large amounts of personal information or causing significant harm, penalties can be further increased. Additionally, Article 285(1) addresses crimes involving unauthorized acquisition, deletion, alteration, or addition of data in computer systems through technical means, with a maximum penalty of five years' imprisonment or

detention, and fines. The Personal Information Protection Law supplements and enhances the Criminal Law's shortcomings in personal information protection through strict administrative and civil liabilities, strengthening comprehensive legal protection. However, there are many issues and challenges in law enforcement. First, the ambiguity of legal provisions makes it difficult to define "illegal use" clearly in judicial practice, complicating enforcement and adjudication. Second, with the continuous development of information technology, new criminal methods emerge frequently, and existing laws lag in addressing complex and evolving illegal activities. Additionally, obtaining and recognizing evidence is particularly challenging, especially concerning cross-border data flows and anonymized information, posing both technical and legal challenges to law enforcement agencies. Finally, the deterrent effect and consistent application of penalties need further strengthening to ensure fairness and effectiveness in law enforcement. In summary, the analysis of criminal liability for the illegal use of personal information demonstrates that while China has established an initial legal framework, further improvement and strengthening in specific application and enforcement processes are needed. Clarifying the constitutive elements of criminal liability, refining legal provisions, and enhancing law enforcement and judicial capabilities can more effectively combat the illegal use of personal information, protect citizens' legitimate rights, and uphold social justice and fairness.

5. Challenges and Issues in Criminal Regulation

Although China has made progress in criminal regulation of the illegal use of personal information, various challenges remain in its practical implementation, necessitating further measures to improve the effectiveness and deterrent power of the law. First, legislative issues are mainly reflected in the ambiguity and incompleteness of legal provisions. Current laws, such as the Criminal Law and the Personal Information Protection Law, lack detailed definitions of illegal use behaviors, leading to potential discrepancies in judicial interpretation. For example, the specific scope and boundaries of "illegal use" are not clearly defined, leaving discretion for law enforcement agencies in identifying criminal behavior. Moreover, the rapid evolution of information technology has given rise to new forms of personal information crime, which current laws are not well-equipped to address, necessitating legislative amendments or supplementary legislation. Second, law enforcement issues are characterized by insufficient enforcement efforts and limited resources. The hidden and technical nature of personal information crimes poses challenges for law enforcement agencies in investigation and evidence collection. Current human, technical, and financial resources in relevant enforcement departments are relatively limited, making it difficult to address increasingly complex information crimes. Additionally, law enforcement personnel require enhanced training in professional knowledge and skills to improve their ability to identify and combat illegal use of personal information. Third, challenges arising from technology and societal development cannot be ignored. The rapid advancement of technologies, such as big data, artificial intelligence, and blockchain, has greatly increased the complexity of personal information protection. Criminals use sophisticated technological

means for data theft, encrypted transmission, and anonymous transactions, posing significant challenges for law enforcement. Moreover, the widespread flow of cross-border data makes international cooperation essential in combating personal information crimes, but differences in legal systems and enforcement standards among countries hinder effective cooperation. Fourth, insufficient legal responsibility and penalties remain a prominent issue. While the Criminal Law and the Personal Information Protection Law stipulate criminal liability for the illegal use of personal information, in practice, the deterrent effect and consistent application of penalties need strengthening. On one hand, existing penalties and sentencing standards may not cover all serious illegal activities, resulting in some offenses not being properly punished; on the other hand, inconsistencies in sentencing and enforcement across regions and agencies weaken the law's unity and authority. Finally, insufficient public awareness and social participation pose a challenge in criminal regulation. Despite the continuous improvement of laws on personal information protection, public awareness and self-protection capabilities remain weak. Many citizens do not prioritize personal information protection in their daily lives, making them vulnerable to information leaks and misuse. Furthermore, effective reporting channels and legal support for citizens who discover illegal use of their personal information are often lacking, hindering timely detection and resolution of related cases. In summary, the criminal regulation of illegal use of personal information faces numerous challenges in legislation, law enforcement, technological adaptation, international cooperation, and public engagement. To enhance the effectiveness of criminal regulation, it is necessary to improve legal provisions, strengthen enforcement capabilities, promote collaboration between technology and law, facilitate international cooperation, and raise public awareness and participation, thereby building a multi-layered, multidimensional personal information protection system that effectively curbs illegal activities and safeguards citizens' rights and social stability.

6. Recommendations for Improving Criminal Regulation

To address the issues and challenges in criminal regulation of the illegal use of citizens' personal information, this paper offers the following recommendations to enhance the effectiveness and deterrence of the law and fully protect citizens' legitimate rights. 1) improve legal provisions by clarifying the specific behaviors and liabilities associated with the illegal use of personal information. Current laws have some vague definitions and ambiguous scopes, which can lead to differing interpretations in enforcement. It is recommended that legislators provide more detailed definitions for behaviors such as "unauthorized acquisition," "illegal sale," and "illegal dissemination" and specify penalties for varying degrees of offense. Additionally, to keep pace with technology, laws should be revised and supplemented to address emerging information crimes, such as big data misuse and AI-driven privacy intrusions. 2) strengthen enforcement and build enforcement capacity. Crimes involving the illegal use of personal information are often concealed and technically complex, necessitating skilled technical personnel and advanced tools for investigation and evidence collection.

Increased funding and resources for law enforcement departments are recommended to improve their ability to handle complex information crimes. Moreover, establishing cross-departmental and cross-regional cooperation mechanisms, enhancing information sharing, and conducting joint actions are essential to creating a coordinated effort to combat the illegal use of personal information. 3) promote collaboration between technology and law. Using advanced technology, such as blockchain, artificial intelligence, and big data analysis, can improve the monitoring and management of personal information flows. It is recommended to establish intelligent monitoring systems for real-time detection and alerts of illegal information use, enabling timely intervention. In addition, the development and application of privacy protection technologies, such as data encryption and anonymization, should be encouraged to reduce the risk of personal information leaks during storage and transmission. 4) strengthen international cooperation and legal coordination. As cross-border data flows become more frequent, a single country's legal measures alone cannot effectively address international information crimes. China should actively participate in the formulation and revision of international data protection regulations and promote information-sharing and enforcement cooperation mechanisms with major countries and regions to jointly combat international information crimes. Bilateral or multilateral data protection agreements should be signed to ensure the legality and security of cross-border data transfers. 5) raise public awareness and encourage social participation. The effective implementation of the law relies on public understanding and support. It is recommended to promote personal information protection through various channels, enhancing citizens' privacy awareness and self-protection abilities. Additionally, the public should be encouraged to participate in monitoring information protection, with convenient reporting mechanisms established for promptly identifying and exposing illegal information use. Government and social organizations should jointly conduct training and educational activities to increase public awareness and understanding of personal information protection laws. 6) improve liability and penalty mechanisms. To enhance the deterrence of the law, the establishment of stricter penalties and liability standards is recommended to ensure sufficient punishment for illegal use of personal information. Laws should provide for harsher penalties, such as increasing maximum prison sentences and fine amounts, especially for cases with severe consequences. Ensuring consistency and fairness in penalties is also essential to prevent discrepancies in law enforcement across regions and departments, thereby upholding the law's unity and authority. In conclusion, by refining legal provisions, strengthening enforcement, promoting technological collaboration, enhancing international cooperation, raising public awareness, and improving penalty mechanisms, China can effectively elevate the criminal regulation of illegal use of personal information. This approach will build a more comprehensive and efficient personal information protection system, fully safeguard citizens' privacy rights and information security, and contribute to societal harmony and stability.

7. Conclusion

This paper systematically explores the issue of criminal regulation on the illegal use of citizens' personal information. It first defines personal information and its classification, analyzes specific forms of illegal use, and compares relevant domestic and international laws, revealing the current status and shortcomings of China's criminal regulation. The study finds that, although the Personal Information Protection Law (PIPL) and related criminal laws provide a legal foundation for combating the illegal use of personal information, significant gaps remain in the refinement of legislation, enforcement efforts, technological responses, and cross-border cooperation. These issues manifest in vague legal provisions, limited enforcement resources, challenges in addressing emerging information crimes, and low public awareness of protection. In response to these issues, this paper offers several recommendations for improving criminal regulation, including clarifying legal definitions and penalties, building enforcement capacity, promoting the integration of technology with law, strengthening international cooperation, and raising public awareness. These measures aim to establish a more effective and efficient personal information protection system, enhancing the deterrence and enforceability of the law and fully safeguarding citizens' privacy and information security. In summary, enhancing criminal regulation of illegal use of personal information is not only essential for protecting citizens' rights but also crucial for fostering a healthy digital society. In the future, a coordinated effort across legislation, enforcement, technology, and public engagement will be necessary to continuously improve the level of personal information protection, ensuring that the legal system keeps pace with technological advancements, thereby promoting social justice and information security.

References

Chang, Y. (2023). Definition of "Personal Information" in the Crime of Infringing on Citizens' Personal Information—From the Perspective of Personal Information Protection Law. *Law and Economy*, *2*(5), 19-26. https://doi.org/10.56397/LE.2023.05.03

Giannakoula, A., Dafni, L., & Maria, K. G. (2020). Combating crime in the digital age: A critical review of EU information systems in the area of freedom, security and justice in the post-interoperability era: Challenges for criminal law and personal data protection. *Brill Research Perspectives in Transnational Crime*, *2*(4), 1-97. https://doi.org/10.1163/24680931-12340010

Oliinyk, O. et al. (2020). The principles of criminal law in the aspect of protection of constitutional rights of citizens. *Amazonia Investiga*, *9*(27), 445-459. https://doi.org/10.34069/AI/2020.27.03.49

Pang, X. Z. (2021). Civil law protection of personal information in the era of big data. *Open Access Library Journal*, *8*(10), 1-12. https://doi.org/10.4236/oalib.1108016

Petrović, D. (2022). Privacy and protection of personal data–criminal law aspect. *Strani pravni život*, *66*(4), 469-489. https://doi.org/10.56461/SPZ_22407KJ

Shanshan, G. O. N. G., & Tao, L. I. (2022). Protection Path of Abusing Citizen's Personal Information by Criminal Law: Taking Personal Health Information as an Example. *Journal of Beijing University of Aeronautics and Astronautics Social Sciences Edition*, *35*(6), 64-71.

Tong, Y. F. (2023). The Influence of the Personal Information Protection Law on Crime Evaluation under the Principle of Law Unity. *China Legal Sci.*, *11*(2023), 110.

Zhang, Y., & Dong, H. Y. (2023). Criminal law regulation of cyber fraud crimes—From the perspective of citizens' personal information protection in the era of edge computing. *Journal of Cloud Computing*, *12*(1), 64. https://doi.org/10.1186/s13677-023-00437-3

Zhao, J. (2023). Reflections on Criminal Compliance for Corporate Personal Information Protection. *Beijing L. Rev.*, *14*(2023), 674. https://doi.org/10.4236/blr.2023.142036

Zhu, F. B., & Song, Z. Y. (2022). Systematic Regulation of Personal Information Rights in the Era of Big Data. *SAGE Open*, *12*(1), 21582440211067529. https://doi.org/10.1177/21582440211067529