

Research on the Defects and Perfection of the Criminal Law Protection of Chinese Citizens' Personal Information Rights

Guanzheng Li*

Law School of Guizhou University of Finance and Economics, Guiyang 550025, Guizhou, China

*Corresponding author: Guanzheng Li, 2045922946@qq.com

Copyright: © 2025 Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), permitting distribution and reproduction in any medium, provided the original work is cited.

Abstract: With the rapid development of technology, humanity has entered the era of big data. Big data technology can accurately identify users' daily needs and push content that interests them. However, while enjoying this convenience, the issue of information leakage has also emerged. Some criminals steal personal information and use it as a tool for illegal profit. As a result, citizens' personal information is virtually exposed to the public, leading to an influx of spam messages and harassing phone calls. This not only disrupts people's lives but also poses a serious threat to their personal and financial security. Therefore, it is urgently necessary to use criminal law to regulate crimes that infringe upon citizens' personal information. To address the shortcomings in China's criminal law regarding personal information protection, this study proposes several suggestions, such as replacing "citizens' personal information" with "personal information", establishing the public nature of legal interests, and adding new forms of criminal behavior. The goal of this paper is to enable criminal law to play its role fully in protecting personal information.

Keywords: Citizens' personal information; Criminal law protection; Crime of infringing on citizens' personal information

Online publication: April 3, 2025

1. Introduction

Regarding personal information protection, the current issues are not only limited to incomplete legal frameworks but also include citizens' lack of awareness and disregard for protecting their own personal information and rights. Therefore, it is urgent to improve personal information protection methods, accelerate legislative advancements, and enhance public awareness of personal information security. This has become increasingly important to ensure better protection of personal information amid the rapid development of the big data era.

2. The importance of strengthening the protection of citizens' personal information

2.1. The normalization of the information leakage trend

In the era of big data, the leakage of personal information has become increasingly normalized, and people have gradually grown numb to it. Rather than embracing openness, they have, in effect, abandoned their rights. Personal information has become the fuel driving the rapid development of big data, with citizens' data making up the largest share. Recognizing its immeasurable value, some countries even refer to personal information as “the oil of the future”, underscoring its critical importance. However, due to inadequate legal protection and citizens' weak awareness of data security, many individuals passively allow their data to be exploited. The perceived inconvenience and high cost of pursuing legal action further discourage people from taking steps to protect their personal information, fueling the rampant spread of data breaches. This highlights the urgent need for stronger regulations on data collection, clear limitations on data usage, and stricter accountability for those who illegally obtain and exploit personal data ^[1]. Without decisive legal intervention, massive leaks of personal information will continue to be the norm. There are two main causes of this issue: First, many individuals fail to protect their data, blindly granting app permissions, filling in extensive personal details, and sharing their locations online, creating opportunities for criminals to exploit and posing significant risks to personal and financial security. Second, many applications excessively collect users' personal data, including search history, browsing history, and credit information, far beyond what people expect. This over-collection has become a widespread norm as companies use the data to build databases and support future business development.

2.2. Threatening the safety of citizens' life and property

Since the beginning of the 21st century, the digital era has experienced rapid development, bringing with it challenges in strengthening information protection. In recent years, cases of personal information infringement have risen annually, leading to public doubts about the government's ability to safeguard personal data ^[2]. As a result, a phenomenon has emerged where people avoid clicking on unknown links or answering calls from unfamiliar numbers due to a deep-seated distrust in personal information protection, believing these are tactics for scams fueled by data breaches. This has left individuals feeling exposed, as if they are walking naked in public. Due to incomplete protection mechanisms, sensitive information may already be in the hands of others, used for illicit financial gain. Once personal data is illegally collected and exploited, individuals are bombarded with spam calls, messages, and emails—often tailored based on their recent activity, showing a direct consequence of the imbalance in data protection. The root cause of these illegal activities lies in personal information leakage, highlighting the urgent need to strengthen criminal law protections for personal data. Such legal measures are not only necessary for legislative integrity but also align with the demands of the times ^[3].

3. The inadequacy of the protection of Chinese citizens' personal information

3.1. The crime of “infringing on citizens' personal information” is not clear

The prevailing view in criminal law holds that the target of a crime refers to the specific person or object directly affected by the criminal act, as explicitly stated in the provisions of the criminal code. Currently, the criminal target of the crime of “Infringement of Citizens' Personal Information” in China's criminal law is “citizens' personal information.” However, the law does not clearly define the scope of “citizens”, leading to ambiguity in the protection range and raising questions about whether the personal information rights of foreigners and stateless persons are safeguarded under Chinese criminal law ^[4]. From a theoretical perspective, the law upholds

the principle of equality, meaning that everyone's personal information rights should be equally protected. From a social development standpoint, China has embraced an open-door policy, and the number of non-citizens residing in China has surged in recent years. If equal protection is not extended to them, it could negatively impact the country's development and social stability. However, the wording of the criminal offense—"Infringement of Citizens' Personal Information"—raises the question of whether the law is intended to protect only Chinese citizens' personal data. In practice, the Supreme People's Court addressed this issue in its 2012 research opinion on Article 253(1) of the Criminal Law, stating that "citizens" in the crime of "Illegally Obtaining Citizens' Personal Information" should not be limited solely to Chinese nationals. This implies that "citizens' personal information" and "personal information" carry no substantial difference, with "citizens" being interpreted in an expanded sense. However, since the term "citizens" in this crime is not explicitly defined in the Criminal Law, it may still be misinterpreted as limiting personal information protection exclusively to citizens, underscoring the need for clearer legal definitions ^[5].

3.2. The legal interest protected under criminal law on citizens' personal information is not accurately defined

China's Criminal Law classifies the crime of "Infringement of Citizens' Personal Information" under the chapter on "Crimes of Infringing on Citizens' Personal and Democratic Rights." This categorization suggests that the crime primarily infringes upon an individual's most fundamental and personal legal interests. However, practical cases have demonstrated that this crime not only violates personal legal interests but also disrupts public and national interests, highlighting an issue with its legal interest positioning ^[6].

First, while the crime's target is personal information, offenders often target an "indeterminate majority" rather than specific individuals. This broad scope of victimization suggests a societal impact beyond personal harm.

Second, the government collects citizens' personal information for regulatory and service purposes. If such information is leaked and the law only considers it a violation of individual rights, the low cost of committing the crime compared to the potential gains creates a disproportionate risk-reward dynamic. This imbalance makes personal information crimes harder to control and can lead to broader social and national issues ^[7].

Third, criminals often package and sell illegally obtained personal information for profit, meaning that this crime also infringes upon property-related legal interests. Therefore, limiting its classification to violations of personal rights is insufficient to capture fully its legal implications. A broader perspective, incorporating aspects of public and economic harm, is necessary for a more comprehensive legal evaluation and effective deterrence.

3.3. The provisions of behavior are not comprehensive

On one hand, in recent years, cases of personal information infringement have surged, yet the Criminal Law does not regulate "illegal use", making it difficult to address cases where information was collected legally but later misused. On the other hand, numerous cases indicate that the primary harm to individuals does not arise during the collection or provision of information but rather during its processing and use. The collection and provision stages often serve only as preliminary steps enabling illegal use ^[8].

On the other hand, compared to the collection and provision stages, the illegal use of personal information poses a more severe threat to legal interests. First, in terms of precision, personal information is inherently identifiable, meaning each piece of data corresponds to a specific individual. When criminals engage in illegal use,

they can easily target individuals with high accuracy, enabling a range of exploitative activities for profit. Second, in terms of direct impact, the harm caused by illegal use is often immediate and direct, whereas the collection and provision stages typically result in only indirect harm. If no subsequent illegal use occurs, the collection and provision of personal data alone do not cause direct harm to the rights and interests of individuals^[9].

4. Suggestions on perfecting the information protection of Chinese citizens

4.1. Replace “citizens’ personal information” with “personal information”

The prerequisite for protecting personal information under criminal law is to first accurately define the scope of “citizens’ personal information.” The author argues that the term “citizen” in the crime of “Infringement of Citizens’ Personal Information” should not be strictly interpreted as referring only to Chinese nationals. Instead, the personal information rights of foreigners and stateless persons should be equally protected. There are two main reasons for this: First, according to the principle of territorial jurisdiction in China’s Criminal Law, if either the act or the consequence of a crime occurs within China’s jurisdiction, Chinese criminal law applies. Therefore, foreigners and stateless persons within China’s jurisdiction should receive the same level of protection as Chinese citizens against personal information crimes^[10]. Second, the 2012 Opinion of the Supreme People’s Court Research Office on Article 253(1) of the Criminal Law explicitly stated that the term “citizen” in the crime of “Illegally Obtaining Citizens’ Personal Information” should include foreigners within China. In the current legal framework, the crime of “Infringement of Citizens’ Personal Information” encompasses not only illegal acquisition but also other forms of infringement. Since there is no justification for treating illegal acquisition differently from other types of infringement, other personal information violations should also adopt the broader interpretation of “citizen.” Therefore, the author suggests that, when appropriate, the crime of “Infringement of Citizens’ Personal Information” should be renamed “Infringement of Personal Information” to avoid misunderstandings regarding the scope of its legal protection^[11].

4.2. Establish the publicity of legal interests

First, the target of this crime is often not a specific individual but rather an indeterminate group of people. Many cases have shown that criminals engage in the bulk trade of personal information, affecting a vast number of victims. This reality surpasses the scope of individual legal interests and meets the public security threat threshold due to its widespread impact.

Second, citizens’ personal information plays an increasingly vital role in economic development, carrying significant commercial value. Criminals obtain and sell this information through various means, which directly infringes on property rights. Since personal information possesses both personal rights and property rights attributes, it is evident that it should not be regulated solely under personal rights protections^[12].

Therefore, although the crime of “Infringement of Citizens’ Personal Information” falls under individual legal interests, it also exhibits characteristics of a public security threat, extending beyond the scope of individual rights protection^[13].

4.3. Add new ways of behavior

In recent years, with the rapid development of society, the demand for citizens’ personal information has surged, giving rise to a gray industry chain of personal information infringement (collection—provision—illegal use). Collection and provision serve as preliminary steps leading to the ultimate stage of illegal use. This establishes

a supply-demand relationship, where regulating only the “supply” (collection and provision) while leaving the “demand” (illegal use) unchecked fails to eliminate the root cause of the problem. If demand remains unchanged while supply decreases, the profitability of trading personal information will rise, further incentivizing criminals to take risks. Therefore, only by incorporating illegal use into criminal law can we achieve comprehensive legal regulation, effectively preventing and punishing such crimes ^[14].

Although Criminal Law Amendment (VII) and Criminal Law Amendment (IX) have gradually improved regulations on the infringement of citizens’ personal information, and subsequent judicial interpretations by the Supreme People’s Court and Supreme People’s Procuratorate have expanded the definition of “illegally obtaining personal information by other means”, these legal provisions still focus only on the collection and provision stages. The lack of regulation on illegal use has led to practical legal loopholes. For instance, e-commerce platforms legally obtain citizens’ personal information but then illegally use it for marketing purposes, such as sending spam messages. Since these businesses initially acquire the information legally, and illegal use is not covered under criminal law, such activities have become increasingly normalized ^[15].

In summary, to effectively combat the crime of the infringement of personal information, illegal use must be explicitly criminalized. Since judicial interpretations cannot create new offenses, as this would violate the principle of legality, the recommended approach is to amend the Criminal Law to introduce a new offense: “Crime of Illegally Using Citizens’ Personal Information.” This amendment would fill existing legal gaps and strengthen the comprehensive protection of personal information.

Disclosure statement

The author declares no conflict of interest.

Reference

- [1] He YF, 2024, Exploring and Perfecting the Protection Path of Personal Information Rights Administrative Law in the Digital Information Age. *Legal System Expo*, 2024(19): 77–79.
- [2] Lu BB, 2024, Binary Integration on the Right Basis of Personal Information Protection in the Digital Age. *Social Science Journal*, 2024(3): 110–119.
- [3] Wu SB, 2024, Define the Boundary of Personal Information Right and Privacy Right from the Particularity of Data Rights. *Modern commerce and Industry*, 2024(10): 200–202.
- [4] Xu K, 2024, Tree of Rights: Theoretical Restatement of Personal Interests of Personal Information. *Social Science, Gansu Province*, 2024(2): 139–150.
- [5] Wang J, 2024, Legal Interests and Rights: Legislative Choice and Value Expression of Personal Information Protection in the Era of Big Data. *Journal of Hubei University of Science and Technology*, 2024(1): 49–56.
- [6] Zheng WY, 2024, On the Balance Between Individual Rights and Public Interest in the Protection of Personal Biometric Information. *Legal Science (Journal of Northwest University of Political Science and Law)*, 2024(2): 159–168.
- [7] Tong YF, 2024, Conflict and Ablation of Blockchain Technology and Personal Information Rights. *Journal of Northeastern University (Social Science Edition)*, 2024(1): 108–116.
- [8] Li HL, 2023, The Obligation of “Consent” for Personal Information Protection under the Rights Theory is Directed to. *Legal System Expo*, 2023(30): 36–38.
- [9] Zhu HC, 2023, The Witness of Personal Information Right under the Concept of Common Good Rights. *Journal of*

Jiangsu Institute of Technology, 2023(5): 60–68.

- [10] Tan YQ, 2023, The Interpretation Theory of the Judicial Realization of Personal Information Subject Rights. *Network Security and Data Governance*, 2023(9): 42–49.
- [11] Song CF, 2023, Analysis of Personal Information Right Bundle and Personal Information Processing Autonomy. *Journal of Wuhan University of Technology (Social Science Edition)*, 2023(3): 1–9.
- [12] Han SY, 2023, Subjective Public Rights in the Protection of Personal Information. *Legal Research*, 2023(4): 87–100.
- [13] Xu HJ, 2023, Research on the Civil Law Protection Specification of Citizens' Personal Information Rights under the Background of Big Data. *Legal System Expo*, 2023(12): 106–108.
- [14] Xu L, 2024, Reduction and Limits of Personal Information Rights in Scientific Research. *Scientific Research*, 2024(2): 240–247.
- [15] Xie DZ, 2023, An Analysis of the Restriction and Protection of Personal Information Rights in Criminal Procedure. *Legal System Expo*, 2023(11): 78–80.

Publisher's note

Bio-Byword Scientific Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.