Science of Law Journal (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2024.030808
ISSN 2616-2296 Vol. 3 Num. 8

Research on the Criminal Law Governance of Crimes Infringing on Personal Information in the Internet Era

Hui Guo

School of Finance and Public Administration, Anhui University of Finance and Economics, Bengbu, Anhui, 233030, China
544082570@qq.com

Keywords: Internet era, crimes infringing on personal information, criminal governance

Abstract: With the widespread application of big data and internet technologies, China has gradually entered a digital society. The characteristics of this digital society directly determine the modes of social connection, production organization forms, and social lifestyles. While the internet era brings convenience to people, it also generates a series of risks, among which the infringement and abuse of personal information rights have become a severe social issue. Therefore, how to seek effective countermeasures to achieve a balance between the healthy and orderly development of the internet and the comprehensive protection of personal information has become a pressing issue in legal research and social governance. In practical terms, attention should be paid to various issues such as the blurred boundaries of crimes infringing on citizens' personal information and the difficulties in defining the standard of "serious circumstances." Strengthening criminal governance over infringements of personal information and clarifying the role of criminal law in the personal information protection system are crucial to laying the foundation for constructing a comprehensive governance system involving multi-party participation to combat the illegal and criminal activities of infringing on personal information.

1. The Importance of Personal Information Protection in the Internet Era

1.1 Safeguarding Personal Privacy Rights

In modern society, personal privacy is one of the basic rights of citizens, and personal information, as an important part of privacy, is directly related to the protection of individual privacy rights. In recent years, with the rapid development of internet technologies, personal information has been widely applied across various fields, from daily shopping to social activities, financial services, and healthcare. However, this convenience also conceals significant risks. If personal information protection is inadequate, privacy breaches are likely to occur, leading to a series of problems[1-2]. Therefore, protecting personal information is a crucial aspect of safeguarding privacy rights, ensuring social stability, and maintaining personal security.

1.2 Promoting Social Harmony and Stability

In today's rapidly developing information society, personal information serves as a critical link between individuals and society. However, the issue of personal information leakage has become increasingly prominent, severely infringing on citizens' privacy rights. In severe cases, it can lead to social conflicts. If personal information is exploited by criminals, it can easily facilitate illegal activities such as harassment and fraud. If victims' legitimate rights and interests are harmed, it will undoubtedly challenge social fairness and justice, arousing public dissatisfaction and anger, thus increasing social instability. Effectively protecting personal information and building a comprehensive protection network are essential measures to maintain social harmony and stability, reducing the risks posed by information leakage and enhancing public trust[3].

2. Characteristics of Crimes Infringing on Personal Information in the Internet Era

2.1 Convenience of Criminal Implementation

The widespread adoption of internet technologies has made it easier for criminals to illegally obtain and transmit personal information, thereby facilitating the commission of crimes. In the internet era, people’s social activities such as work, study, travel, and consumption are conducted online, where personal information is widely used. Criminals, using techniques like hacking, can easily access personal information from the internet, collect citizens' data, and sell it for profit. For instance, in the case of Ding Yaguang’s personal information infringement, the criminals exploited system vulnerabilities, downloading personal data from illegal websites and selling it through their websites.

2.2 Multiplicity of Criminal Actors

The perpetrators of personal information crimes are not limited to individuals; legal persons or organizations can also be criminal actors driven by profit to illegally obtain, sell, or provide personal information. The crime of infringing on personal information has a general actor, meaning anyone with criminal responsibility can commit the offense, including organizations[4]. For example, in cases of illegal provision or sale of personal information, perpetrators might exploit their job positions to obtain and sell data. Some crime groups have fixed roles, with members specialized in information acquisition and well-organized, as illustrated in Figure 1. Public servants and corporate employees are high-risk groups involved in the sale of personal information, as their roles often grant them access to large volumes of data, making them a source of such crimes.

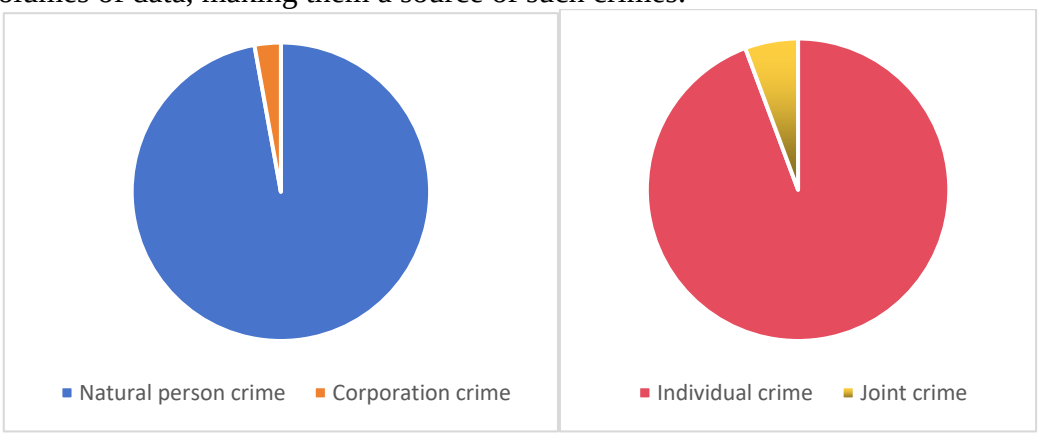

Figure 1: Analysis of the Typology of Criminal Actors in Personal Information Crimes

2.3 Diversity of Criminal Behavior

The prevalence of online payments and the professionalization of hacking technologies make cross-regional crimes easier to commit. Offenders can conceal their identities and actions within virtual networks. In many cases, personal information crimes are carried out by organized groups, where members have distinct roles[5]. They may advertise the sale of personal information through social media platforms like WeChat, conduct transactions online using virtual identities, and then disappear by deleting their profiles, making it difficult for law enforcement to track them. The rapid dissemination of such advertisements can lead to widespread harm, with significant social consequences. The commercialization and industrialization of personal information crimes pose severe threats to citizens' safety, as information trading platforms, including websites, cloud storage, and messaging apps, become the "conveyor belts" for these illegal activities.

3. Trends in Crimes Infringing on Personal Information in the Internet Era

3.1 Increasing Crime Numbers

With the advent of the internet era, the application and commercial value of personal information have become increasingly evident, leading to a surge in crimes involving personal data. In the field of telecommunications fraud, it is common to see the misuse of personal data such as identity card numbers and phone numbers. A search of legal databases using keywords like "personal information infringement" and "crimes infringing on personal information" from 2016 to 2021 yielded 9,150 related cases. In 2016, there were 302 cases; in 2017, 1,151; in 2018, 2,018; in 2019, 2,419; in 2020, 2,131; and in 2021, 1,129. These figures indicate that since the establishment of the crime of personal information infringement in 2015, cases have steadily increased, peaking in 2019, and declining thereafter. Nonetheless, the overall trend shows a significant increase, with widespread infringement of personal information remaining a serious issue as shown in Figure 2.

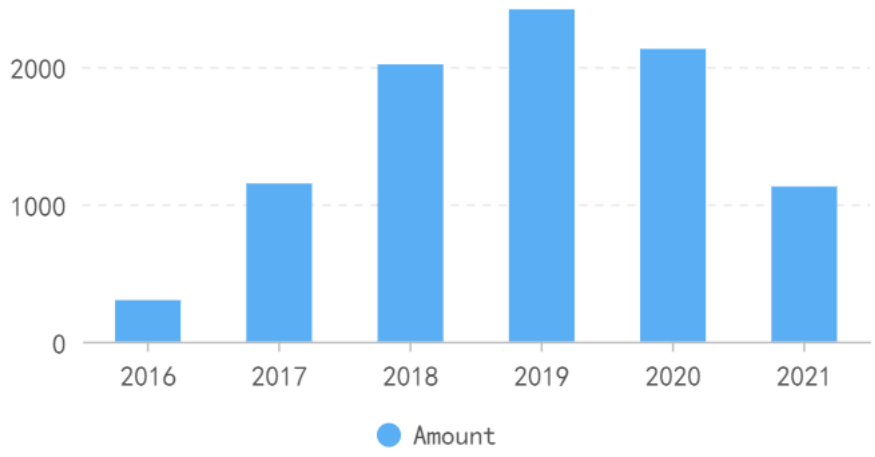

Figure 2: Number of Crimes from 2016 to 2021

3.2 High Social Harm

In the context of the internet era, the digitalization of society has led to a multidimensional evolution of personal information crimes. Digital logic shapes people’s thinking and lifestyles, and

the rapid circulation and sharing of information create a space for the misuse of personal data. The commercial application of personal information in the digital age further incentivizes the misuse of others' data. As people participate in social life and receive services, they inevitably provide personal information, bringing about associated risks. The deeper and broader the social connections, the greater the potential risk to personal information security. The value of personal data in areas such as advertising, tracking, and identity verification increases the risks of infringement[6-7]. The pursuit of economic interests or the intent to commit targeted crimes fuels the proliferation of personal information crimes, jeopardizing the safety, property, and privacy of large populations.

3.3 Technologization of Criminal Behavior

With the continuous advancement of information technology, the methods of committing personal information crimes have evolved, shifting from traditional methods like exploiting job positions to technological and intelligent approaches. For instance, web scraping, which uses automated techniques to extract data from internet platforms, has become a typical means of obtaining personal information. Techniques such as automated CAPTCHA recognition, data decryption, and proxy IP pools are employed to amass personal data for specific purposes. The deep mining of personal information has also become closely linked to advances in artificial intelligence and algorithmic improvements, significantly enhancing the precision and applicability of this data. The unique nature of cyberspace amplifies the technical sophistication of these crimes. As technology develops, perpetrators continuously adopt new techniques to maximize illegal profits.

4. Criminal Law Governance Strategies for Crimes Infringing on Personal Information in the Internet Era

4.1 Clarifying the Role of Criminal Law

Table 1: How to Clarify the Role of Criminal Law in the Protection of Personal Information

Methodology	Detailed content
Strengthening the Leading Role of Criminal Law	By means of legislation, clearly establish the primary role of criminal law in protecting citizens' personal information, ensuring that criminal law has sufficient deterrence and enforceability in combating crimes that infringe on personal information.
Coordinating with Other Legal Systems	Criminal law should be coordinated with other legal norms (such as moral norms, administrative legal norms, and civil legal norms) to avoid conflicts and redundancies, ensuring the integrity and consistency of the legal system.
Narrowing the Scope of Adjustments	When criminal law intersects and overlaps with other legal norms, it should minimize its scope of adjustment, avoiding excessive intervention and punishment, ensuring fairness and reasonableness in the legal system.
Clarifying the Conditions for the Application of Criminal Penalties	Through judicial interpretation and case law guidance, clarify the conditions for the application of criminal penalties in protecting citizens' personal information, ensuring the accuracy and fairness of criminal penalties.

In today's social context, personal information has transcended its original recording function and

is now closely tied to personal safety, property security, and other critical matters. Information risk has become a common and unavoidable reality. If the infringement on personal information intensifies, it will inevitably affect social stability, and the state must take responsibility for risk governance. Criminal law, being the most powerful tool with the most noticeable governance effects, must respond quickly, as shown in Table 1. The practice of governing crimes infringing on personal information in China has demonstrated that criminal law has always led other laws, playing a dominant role in legislation for the protection of personal information. However, criminal law is only one part of the legal system. While maintaining its independence, it must also exercise restraint in interacting with other legal norms, including moral, administrative, and civil laws. When criminal law intersects and overlaps with these norms, its scope should be minimized, avoiding the use of punitive measures unless absolutely necessary.

4.2 Scientifically Defining Criminal Responsibility

The purpose of punishment is to prevent crime, but its ideal effect cannot be achieved merely through enactment, application, and enforcement. Criminal penalties serve deterrent, compensatory, and educative functions, with the overall goal of crime prevention achieved through these social effects[8]. In cases involving the crime of infringing on personal information, fines should be the primary form of punishment. The advantage of fines is that they do not deprive the offender of personal freedom, allowing them to avoid incarceration and continue contributing to society. This reduces the burden on their families and promotes social reintegration. Moreover, fines are low-cost and involve minimal execution risks. Non-penal measures should also be considered. Since the crime involves personal information, which is private and can cause psychological harm to victims, non-penal responses such as warnings, public apologies, or compensation for damages could reduce the likelihood of recidivism.

4.3 Establishing Third-Party Supervisory Agencies

Both government and commercial entities tend to handle personal information within their internal operations. For individuals whose rights have been violated, it can be difficult to detect the breach in a timely manner. Therefore, an authoritative, legally empowered third-party agency should be established to supervise personal information processing and provide expert services. Many countries have already included provisions for independent third-party supervisory agencies in their legislation. For example, Article 36 of Iceland’s Personal Data Protection Act states that the Personal Data Protection Authority should be an independent body with its own committee. China can draw on this experience, ensuring that supervisory bodies are consulted when formulating administrative measures or regulations related to personal information rights and obligations, thus maximizing the protection of personal privacy.

4.4 Ensuring the Normal Flow of Personal Information

The internet’s openness and sharing enable the full realization of information exchange, which in turn drives social progress. However, the demand for personal information protection, from the perspective of safeguarding citizens' rights, often conflicts with the public interest in the free flow of information. In the information society, personal information resources are limited, and there is an inherent tension between an individual’s exclusive rights to their data and society’s need for information[9-10]. Excessive emphasis on exclusivity can hinder the free flow of information, limiting public access and impeding information exchange. Striking a balance between protecting personal data and promoting the free flow of information has become a challenging task. When personal data

is overprotected, it can suppress the free flow of information. Thus, legislation on the protection of personal information in the internet age must strike a balance—preventing the infringement of individual rights while avoiding excessive restrictions on data sharing[11].

5. Conclusion

In the context of the internet era, while it has brought considerable convenience to people's work and lives, the issue of personal information infringement has been amplified and has drawn widespread attention. The protection of personal information is of paramount importance, both in theoretical research and in legislative and judicial practice. Given the current trends, the characteristics of low-cost, low-risk, and high-reward crimes have driven many to target citizens' personal information. To curb the high incidence of such crimes, personal information has been incorporated into the scope of criminal law protection, offering the strongest form of protection. Therefore, it is necessary to learn from foreign legislative experiences, synthesize domestic scholars' theories on the legal protection of personal information, and address issues that arise in judicial practice. From an institutional perspective, providing feasible recommendations for enhancing the criminal law protection of personal information can pave the way for comprehensive governance of such infringements.

References

[1] Ni, Q., Guo, J., Wu, W., & Wang, H. (2022). Influence-Based Community Partition With Sandwich Method for Social Networks. IEEE Transactions on Computational Social Systems, 1–12. https://doi.org/10.1109/TCSS.2022.3148411.

[2] Yusoff AM, Salam S, Mohamad S, Daud R (2017) Gamification Element through Massive Open Online Courses in TVET: An Analysis Using Analytic Hierarchy Process. Journal of Computational and Theoretical Nanoscience, 23(9): 8713–8717.

[3] Cao K, Wang B, Ding H, Lv L, Dong R, Cheng T, Gong F (2021) Improving Physical Layer Security of Uplink NOMA via Energy Harvesting Jammers. IEEE Transactions on Information Forensics and Security, 16:786–799. https://doi.org/10.1109/TIFS.2020.3023277.

[4] Hurley JS (2017) Quantifying Decision Making in the Critical Infrastructure via the Analytic Hierarchy Process (AHP). International Journal of Cyber Warfare and Terrorism, 7(4):23–34.

[5] Sood AK, Talluri S, Nagal A, Ruthvik Reddy SL, Bharathasimha RD, Chaturvedi R (2021) The Covid-19 threat landscape. Computer Fraud & Security, 2021(9):10–15.

[6] Ooi J, Promentilla M, Tan RR, Ng DKS, Chemmangattuvalappil NG (2018) Integration of Fuzzy Analytic Hierarchy Process into multi-objective Computer Aided Molecular Design. Computers and Chemical Engineering, 109(JAN.4): 191–202.

[7] Singh SP, Prakash T, Singh VP, Babu MG (2017) Analytic hierarchy process based automatic generation control of multi-area interconnected power system using Jaya algorithm. Engineering Applications of Artificial Intelligence, 60(Apr.):35–44.

[8] Jiang H, Dai X, Xiao Z, Iyengar AK (2022) Joint Task Offloading and Resource Allocation for Energy-Constrained Mobile Edge Computing. IEEE Transactions on Mobile Computing. https://doi.org/10.1109/TMC.2022.3150432.

[9] Vayansky I, Kumar S (2018) Phishing – challenges and solutions. Computer Fraud & Security, 2018(1):15–20.

[10] Santis R, Golliat L, Aguiar E (2017) Multi-Criteria Supplier Selection using Fuzzy Analytic Hierarchy Process: Case Study from a Brazilian Railway Operator. Brazilian Journal of Operations & Production Management, 14(3):428–437.

[11] Ahmed S, Vedagiri P, Rao KK (2017) Prioritization of pavement maintenance sections using objective based Analytic Hierarchy Process. International Journal of Pavement Research and Technology, 10(2):158–170.