ISSN 2616-7433 Vol. 7, Issue 4: 10-17, DOI: 10.25236/FSST.2025.070402

The Construction of the Relationship between the Chinese Government and Public Trust: A Case Study of Online Personal Information Security

Lin Li

Department of Political Science and International Studies, Incheon National University, Incheon, 22012, Republic of Korea
li1537310883@163.com

Abstract: *The proliferation of the internet and the rapid evolution of an information-driven society have resulted in the widespread collection and storage of personal data in daily life. In China, the issue of personal information security in cyberspace has become a key factor influencing the trust relationship between the government and its citizens. Data breaches and the misuse of personal information not only infringe upon individual privacy rights but also undermine public confidence in governmental credibility, governance capacity, and political legitimacy. This study examines the privacy challenges faced by citizens in the digital era from the perspective of online personal information security and explores their implications for the construction of governmental trust. It argues that restoring and reinforcing public trust requires effective measures such as enhancing transparency, strengthening accountability, refining legal and regulatory frameworks, and promoting international cooperation in the field of information security.*

Keywords: *government, citizens, trust, network, information*

1. Introduction

The global trend toward informatization is accelerating, with internet technologies increasingly permeating all facets of public life. The speed and breadth of information dissemination are expanding continuously, accompanied by an exponential increase in data generation, storage, and transmission. The widespread application of information technology has not only driven economic growth and social development but also fundamentally reshaped human behavior and the structure of national governance. The internet now plays a central role in contemporary society, encompassing domains such as e-commerce, social networking, and the expansion of e-government services. As information becomes a critical asset, its security directly affects national security, corporate competitiveness, and individual privacy.

At the national level, information security has evolved beyond a purely technical or corporate concern into a critical issue of public security, closely tied to social stability, political governance, and economic prosperity. At the individual level, it directly impacts personal privacy rights and the protection of private property. The frequent occurrence of security breaches has exposed significant vulnerabilities in cyberspace, revealing challenges that extend beyond technical limitations. These issues represent a comprehensive test of governmental legitimacy, corporate credibility, and public trust [1].

Safeguarding information security is both a technological imperative and a political responsibility. Governments bear a dual obligation: to protect the state and its citizens from cyber threats, and to cultivate public trust in their management of cybersecurity. As threats escalate, citizens increasingly scrutinize the state's capacity for effective governance in this domain. Persistent cyberattacks, data breaches, and violations of privacy contribute to the erosion of trust, while global discourse surrounding state surveillance, citizen privacy, and data protection grows more contentious.

In light of these dynamics, this study addresses two central questions: How do information security concerns affect individuals' trust in government? And how can governments formulate effective policy frameworks that safeguard cybersecurity while concurrently enhancing public trust—thus achieving a sustainable balance between these imperatives?

ISSN 2616-7433 Vol. 7, Issue 4: 10-17, DOI: 10.25236/FSST.2025.070402

2. Personal information security and issues related to citizens

To understand the relationship between personal information security and public trust, it is essential to first define information security. Information security refers to a set of protective measures aimed at safeguarding data as well as the systems and hardware involved in its storage, transmission, and utilization. Its primary objectives are to ensure the availability, accuracy, authenticity, confidentiality, integrity, usability, and ownership of information [1]. Information security threats are defined as any conditions or events that increase the likelihood of information being compromised, manipulated, or attacked [1].

Personal privacy information includes sensitive data such as bank account details, phone numbers, national identification numbers, residential addresses, email accounts, social media credentials, financial status, and consumption patterns. The breach or misuse of such data can inflict both economic and psychological harm on individuals, while also constituting a serious violation of their privacy rights and informational autonomy.

Therefore, the protection of personal information is of critical importance. The effective implementation of national information security policies can significantly enhance citizens' trust in both public institutions and private organizations. Conversely, incidents of data leakage can lead to a decline in public confidence, undermining not only citizens' willingness to participate in political processes but also their overall relationship with the government.

According to data from the China Internet Network Information Center (CNNIC), the number of internet users in China reached approximately 1.1 billion (1.09967 billion) as of June 2024, corresponding to an internet penetration rate of 78.0%. This figure continues to rise steadily. The swift advancement of the digital economy has presented novel issues in personal information security and internet governance, leading to increased public apprehension about the safekeeping of personal data. Citizens' primary concerns regarding personal information security mainly focus on privacy protection, data breaches, civil rights, and the transparency of information usage.

2.1 Privacy protection

What constitutes privacy? Privacy refers to an individual's right to autonomously select which personal information may be accessed by others, when it may be accessed, and how it may be used [2]. This notion involves the regulation and administration of information dissemination and utilization, guaranteeing that individuals maintain decision-making power throughout the information processing continuum.

The growing amount of personal information gathered in the digital realm, along with improved information retrieval, tagging, and aggregation capabilities, has led users to express increased apprehension regarding the potential exposure of their data online [3]. The advent of the big data era has not only endowed personal information with enormous economic worth but has also progressively characterized it with explicit property-like features. This shift has rendered personal information a primary target for criminals aiming to monitor, acquire, and perhaps trade such data [4].

The rise of social networking platforms can be understood through the framework of Habermas's concept of the "public sphere." The public sphere denotes an area positioned between the state and society, where citizens can openly share information and viewpoints [5]. The fundamental goal is to promote open, logical discussion on issues of public concern. The public realm necessitates fundamental rights, such as freedom of expression, freedom of assembly, and the right to engage in political discourse and decision-making [6]. The advent of online social networks has significantly broadened the scope of the public sphere from local to global dimensions. Social media allows individuals to overcome time and spatial limitations, participating in public debate and deliberation, thus creating a novel "digital public sphere."

During this digital transition, individuals increasingly engage in multiple social media platforms (e.g., Sina Weibo), where they share personal experiences and discuss diverse public and political matters. By seeing and participating in these debates, users articulate and share their perspectives, political positions, and interests. The interactive characteristics of these platforms augment the development and distribution of public opinion.

Nonetheless, other privacy-related issues arise during this procedure. Users are typically required to complete a mandatory registration process before being permitted to post or comment publicly [7][8].

ISSN 2616-7433 Vol. 7, Issue 4: 10-17, DOI: 10.25236/FSST.2025.070402

Registration often entails the disclosure of sensitive personal data, including real names, gender, phone numbers, income, educational background, email addresses, and personal biographies [9][10]. Moreover, identity verification via phone or email is frequently required.

Many citizens express apprehension over the potential misuse or unauthorized dissemination of such confidential information. There is a growing expectation that legal frameworks will articulate explicit, enforceable mechanisms for protecting individual privacy and preventing the abuse of personal data.

2.2 Data breach

Data breaches refer to incidents in which sensitive, protected, or confidential personally identifiable information (PII) is accessed, stolen, or misused by unauthorized entities [11]. As previously discussed, citizens' daily lives are increasingly mediated by the internet and a vast array of digital platforms. This has resulted in a substantial rise in the volume and frequency of personal data collection, processing, and storage. Personal data is no longer confined to the private realm; rather, it has evolved into a valuable resource that can be utilized for diverse purposes by various actors. Governments may harness personal data to monitor individual behavior, identify patterns, and oversee public discourse. In parallel, corporations deploy data analytics to examine consumer behavior, anticipate market trends, and implement highly targeted marketing strategies.

Thus, data has evolved into a strategic asset that extends political and economic power. Simultaneously, it can serve as a tool of social control, posing potential threats to individual freedom, privacy, and autonomy.

2.3 Civil rights and information transparency

In the digital era, many individuals increasingly seek clarity regarding the specific purposes for which their personal information is collected, stored, and used by governmental or other entities—particularly in the wake of frequent data breaches. While democratic societies emphasize the protection of privacy through institutional frameworks, they must also enact appropriate regulations that mandate the disclosure of essential public information, all within reasonable and responsible limits [2].

Simultaneously, citizens are asserting a growing demand for control over the collection and utilization of their personal data. This includes key rights such as the right to be informed—which guarantees transparency prior to data collection; the right to erasure—which enables individuals to delete personal data that has already been collected; and the right to rectification—which allows for the correction of inaccurate or outdated information [12]. Citizens increasingly expect that these rights will not only be legally safeguarded but also progressively expanded—empowering them to monitor, manage, and govern the lifecycle of their personal information. This participatory model of data governance corresponds with the concept of "privacy self-management" [13], which posits that individuals should retain agency over the dissemination and processing of their personal information, rather than having it handled in opaque or exploitative ways.

In summary, public concerns regarding personal data encompass a range of issues, including privacy protection, the risks of data breaches, the defense of individual rights, and the demand for greater transparency. In response to these growing complexities, it is imperative for governments to adopt proactive and effective policies that address public anxieties and contribute to the construction of a more secure and trustworthy digital environment.

3. Issues of citizen trust and information security

3.1 Citizen trust

The "citizen trust" mentioned in this article refers to the confidence citizens possess in the government, also known as governmental trust. Government trust pertains to the public's anticipations regarding political leaders and governmental institutions in meeting obligations, exhibiting conduct, and executing responsibilities [14]. In democratic systems, citizens anticipate governmental accountability for all functions and decisions, ensuring effective responsiveness to public needs and actions in the majority's interest [15]. Effective governance practices—particularly regarding responsiveness, accountability mechanisms, and transparency—are crucial for fulfilling public

ISSN 2616-7433 Vol. 7, Issue 4: 10-17, DOI: 10.25236/FSST.2025.070402

expectations [14]. Thus, the efficacy of a democratic system is intricately linked to the trust citizens bestow upon their government. Therefore, governments should endeavor to cultivate and sustain public trust by proficiently executing policies and strategies aimed at addressing citizens' needs [14].

This phenomenon can be analysed via the framework of Jean-Jacques Rousseau's (1712–1778) Social Contract theory, an fundamental concept in political science. The theory posits that state legitimacy derives from the collective consent and endorsement of its citizens, embodied in the concept of the "General Will" [16]. Citizens hope that the state will execute its essential duties, encompassing the safeguarding of individual rights, the preservation of social order, and the advancement of the collective welfare. Within this theoretical framework, the government is expected to demonstrate a significant level of accountability to maintain the essence of the social contract, thereby guaranteeing societal harmony and stability. Public trust in government stems from its perceived ability to fulfil its responsibilities and uphold societal order. In democratic states, civic trust is regarded a critical factor in ensuring social stability and governmental legitimacy. It signifies both citizens' acknowledgement of governmental power and legitimacy, as well as their endorsement of the overarching political system and its governing institutions. The formation of public trust depends on the transparency of governmental activities, the equity of public policy, and the dependability of public institutions. When citizens believe that the government adequately protects their rights and interests, their faith in the state markedly increases.

Consequently, the intricacy of information security challenges, combined with the government's insufficient response, frequently undermines public trust. When personal data is compromised, privacy rights are infringed, or cyberattacks are prevalent, citizens are inclined to question the government's ability to safeguard cybersecurity and may also doubt the integrity and accountability of its institutions.

3.2 The erosion of citizens' trust in government

Public trust is regarded as a crucial pillar of modern governance systems. It serves as a cornerstone of governmental legitimacy and plays a vital role in maintaining social order and fostering public cooperation. However, the recurring incidence of information security breaches is gradually eroding citizens' trust in governments, corporations, and social institutions. This erosion of trust not only undermines the effectiveness of governance but may also pose significant risks to national stability and sustainable development.

3.2.1 Data breaches and cyber attacks

The advancement of information technology has significantly enhanced convenience and entertainment in individuals' lives; however, it has also been accompanied by a notable increase in cyberattacks and data breaches. This phenomenon underscores the multifaceted impact of technological progress and reveals the inherent vulnerabilities of cyberspace. Hacking, malware intrusions, virus infections, spyware deployment, unauthorized eavesdropping and surveillance, robocall harassment, and manipulative tactics can all lead to incidents of identity theft. Such breaches may result in the unauthorized disclosure of personally identifiable information, financial data, and health records [17]. An increasing number of individuals perceive their personal information as being exposed to heightened security risks.

In recent years, major data breaches across the globe have drawn considerable public and academic attention. In 2017, for example, the American credit reporting agency Equifax suffered a cyberattack that compromised the personal data of approximately 143 million U.S. citizens. Similar incidents have occurred not only in the United States but also in many other countries. The widespread exposure of personal information poses significant risks to individual privacy and security, while simultaneously undermining public trust in both governmental institutions and private corporations. In the aftermath of such events, the public often questions the government's administrative competence, as well as the speed and transparency of its response.

3.2.2 Conflict between citizens' privacy and national security

Information security issues can entail tensions between individual privacy and national security. Under the pretext of safeguarding national interests, governments may expand data surveillance and information-gathering efforts. Particularly in areas such as counterterrorism, cybercrime prevention, and international security, data monitoring is frequently regarded as a necessary preventive measure [18]. Michel Foucault's concept of the Panopticon and Mark Poster's elaboration on it through the idea of the Superpanopticon provide valuable frameworks for understanding contemporary surveillance and

ISSN 2616-7433 Vol. 7, Issue 4: 10-17, DOI: 10.25236/FSST.2025.070402

the erosion of public privacy. Foucault's Panopticon model describes a method of social control in which prisoners are isolated but constantly visible to guards stationed in a central tower. Although the inmates cannot see their observers, the omnipresent possibility of being watched compels them to self-regulate and conform to institutional rules—even in the absence of direct supervision [19]. The Panopticon thus serves as a metaphor for modern society's condition of internalized surveillance [20]. Expanding upon Foucault's theory, Mark Poster introduces the concept of the Superpanopticon to characterize the information society, where complex networks of power employ covert technological means to observe the public. In this context, power operates through the management of "attention," requiring individuals under surveillance to adapt to a persistent state of being watched [21].

In the age of big data, the "observer" is often concealed within algorithmic systems, leaving users largely unaware of the surveillance to which they are subjected. Continuous data-tracking technologies facilitate constant, real-time monitoring, thereby eliminating the temporal and spatial limitations associated with traditional forms of surveillance. These advanced surveillance mechanisms are not only instantaneous but also capable of systematically recording and storing data, ensuring the completeness and traceability of surveillance information. State surveillance has expanded into virtual cyberspace and permeated broader society, resulting in increasingly blurred and diversified roles between the "observed" and the "observers" [22].

Information surveillance has increasingly evolved into an extension of governmental authority in modern society. Governments employ advanced technologies to comprehensively monitor individual behavior, thereby maintaining social order and reinforcing state control [23]. As surveillance technologies continue to advance, the state is able to monitor and record citizens' daily activities in more covert and systematic ways. However, the concurrent demands for both security and personal freedom have rendered the protection of privacy more complex and challenging. Even when citizens, under specific circumstances, implicitly consent to the collection of their personal data, many still harbor concerns, viewing such consent as a concession made under the pressures of state governance. The right to privacy is a fundamental safeguard of modern democratic governance, and excessive government surveillance may give rise to a "surveillance state," in which citizens become "digital prisoners."

3.2.3 Delayed laws

China has lagged behind in establishing a comprehensive legislative framework for personal information protection, thereby failing to adequately address the challenges posed by the rapid development of information technology. The specific manifestations of this issue can be summarized as follows.

First, the existing legal framework often fails to keep pace with the escalating risks associated with technological advancements. The widespread adoption of technologies such as big data, artificial intelligence, and blockchain has significantly increased the complexity of collecting, storing, and processing personal information. However, China's personal information protection regime remains largely centered on individual safety, without sufficiently addressing the privacy risks emerging from these evolving technologies. As a result, the protection of individual rights and interests remains inadequate [12][24].

Secondly, insufficient enforcement of current legislation is another major factor impeding the advancement of personal information protection. Despite the introduction of key legislative measures, including the Cybersecurity Law and the Personal Information Protection Law of the People's Republic of China, significant practical challenges persist due to insufficient regulatory oversight and weak enforcement mechanisms. Regulatory agencies often fail to respond promptly to data security breaches, thereby diminishing the deterrent effect of the legal framework. Additionally, the penalties imposed for violations of personal information protection laws are frequently too lenient to serve as an effective deterrent. Consequently, businesses and organizations often operate without sufficient legal constraints to ensure the proper management of personal data [25].

Third, certain illicit cyber organizations engage in the unauthorized registration, collection, and even theft of personal information through various network techniques. Alarmingly, some professional cybersecurity software has also been exposed for unlawfully obtaining users' sensitive data [7]. In addressing these challenges, regulatory agencies have often failed to effectively fulfill their oversight responsibilities, resulting in the recurrent and unrestrained occurrence of violations. The lack of a comprehensive accountability framework has further exacerbated problems related to personal information breaches and unlawful data transfers, significantly infringing upon citizens' privacy rights and eroding public confidence in both the legal system and regulatory institutions.

ISSN 2616-7433 Vol. 7, Issue 4: 10-17, DOI: 10.25236/FSST.2025.070402

4. The government's responsibility and the rebuilding of citizen trust

4.1. The enhancement of information transparency and government accountability

In the realm of information security, transparency and accountability are vital for the government. Re-establishing public trust necessitates assurance in the prudent administration of people' personal data, with any issues requiring rapid and transparent resolution. The government should undertake the following measures. First, it must enhance the transparency of information security incidents to ensure that the public is promptly and accurately informed of the relevant facts. Second, it should promote greater public participation in the development and implementation of information security policies, thereby ensuring that such policies are responsive to the needs and interests of citizens. Third, the government must establish and strengthen robust accountability mechanisms to guarantee that officials and relevant departments are held appropriately responsible when security breaches occur.

4.2. Formulation and improvement of information security policies

The government must establish a comprehensive information security policy framework to address the increasingly complex challenges emerging in cyberspace. In designing this framework, the government should move beyond a narrow focus on technical defense measures and instead integrate institutional, legal, and societal dimensions to ensure that national security is upheld while the privacy rights of citizens are effectively protected. Accordingly, policy development should emphasize not only technological safeguards but also the formulation of robust institutional norms for personal data protection. This entails enhancing individuals' rights to be informed about and to exert control over the utilization of personal data.

The General Data Protection Regulation (GDPR) enacted by the European Union is an internationally acknowledged regulatory benchmark in data privacy protection. The General Data Protection Regulation (GDPR) explicitly delineates the parameters of personal data through legal statutes and outlines comprehensive regulations about the rights and obligations of principal stakeholders, including data subjects, data controllers, and data processors. These legal measures provide robust support for the safeguarding of people' privacy rights and the legitimate transfer of cross-border data [26]. The success of the GDPR offers valuable practical experience for countries worldwide in striking a balance between privacy protection and information security. Drawing on this experience, the Chinese government can incorporate similar effective practices into its policy framework to ensure that data processing activities meet the fundamental requirements of citizen privacy protection. This, in turn, would help strengthen public trust in the government's information security measures.

4.3 International cooperation and global governance of cyberspace

The worldwide scope of information security issues has introduced unparalleled complexity for governments. With the rapid advancement of information technology, cyberspace has increasingly become a new arena for competition and strategic rivalry among nations. The threats linked to cross-border data flows are increasing, frequently surpassing national borders and impacting global regions. The efforts of a single nation are insufficient to comprehensively and effectively address the complex and transnational nature of modern information security threats. Given this context, national governments must strengthen transnational collaboration and establish multilateral cooperation structures in the field of information security. This is especially important for defining rules for cyberspace governance, controlling cross-border data flows, improving information sharing, and implementing coordinated defence strategies—all of which require agreement and collaborative action.

5. Conclusion

Scientific and technical growth, as a crucial driving force in human society's advancement, has considerably enhanced quality of life and boosted economic development. However, it has also had a number of significant negative effects [19]. The rapid development of information technology has significantly enhanced citizens' work efficiency and daily convenience; however, it has also given rise to numerous issues, such as privacy breaches and information security risks. At the same time, the misuse of data, the unauthorized collection and dissemination of personal information, and the growing complexity of cybersecurity threats highlight the need to establish a more comprehensive dual-

ISSN 2616-7433 Vol. 7, Issue 4: 10-17, DOI: 10.25236/FSST.2025.070402

regulatory framework that combines legal instruments with technological measures.

As a fundamental pillar of modern state governance, public trust is essential to the effective functioning of governments and public institutions. It not only shapes citizens' acceptance and endorsement of governmental policies but also constitutes a vital source of political legitimacy. However, the increasing frequency of cybersecurity breaches has progressively undermined public confidence in the government's capacity to ensure information security and safeguard individual privacy—especially when state actions are perceived as insufficiently protective or lacking in transparency. Given the multifaceted nature of information security, it is imperative for governments to strike a careful balance between national security imperatives and the protection of citizens' privacy rights. Ensuring that both national interests and individual freedoms are preserved in the face of cyber threats requires robust, transparent, and accountable institutional responses.

The protection of citizens' personal information depends not only on national-level legal and technological interventions but also on the active engagement of individuals. Nevertheless, many citizens demonstrate insufficient awareness of privacy issues and lack the requisite skills for effective self-protection. Although public concern about internet privacy has grown, the "privacy paradox" remains evident: individuals voluntarily or inadvertently disclose personal information while simultaneously failing to adopt appropriate protective measures [3]. This paradox highlights a significant disconnect between citizens' awareness of information security and their actual behavior. Therefore, governments and relevant institutions should enhance public awareness of information security through structured educational initiatives and targeted outreach efforts. Concurrently, individuals must take an active role in acquiring essential technical competencies and adhering to best practices in cybersecurity—such as utilizing strong, unique passwords and regularly updating and optimizing privacy settings—in order to mitigate the risk of data breaches and more effectively safeguard their legal rights.

References

[1] Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security. Behavior & Information Technology, 29(3), 221–232.
[2] Westin, A. F. (2003). Social and Political Dimensions of Privacy. Journal of Social Issues, 59(2), 431–453.
[3] Young, A. L., & Anabel, Q.-H. (2013). PRIVACY PROTECTION STRATEGIES ON FACEBOOK: The Internet privacy paradox revisited. Information, Communication & Society, 16(4), 479–500.
[4] Chen, Y., & Cheng, P. (2019). Analysis of New Threats to Personal Information Security in the Era of Big Data and Protection. China Management Informationization, 22(04), 164–165.
[5] Castells, M. (2008). The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance. The ANNALS of the American Academy of Political and Social Science, 616(1), 78–93.
[6] Kellner, D. (2000). Habermas, the public sphere, and democracy: A critical intervention. Perspectives on Habermas, 1(1), 259–288.
[7] Zhao, H. (2021). Research on the protection of citizens' privacy in the Internet era. Legality Vision, 31, 15–16.
[8] Li, Z. (2023). Research on the legal protection of personal information in the Online Environment. Journal of Handan University, 33(02), 74–78.
[9] Kayes, I., & Iamnitchi, A. (2017). Privacy and security in online social networks: A survey. Online Social Networks and Media, 3, 1–21.
[10] Ping, Y. (2024). Research on personal information protection based on cyberspace security. Cyberspace Security, 15(04), 47–51.
[11] Adebayo O Adewale. (2018). Data Breach Risk Reduction through Perimeter Security and Smart Surfing. International Journal of Computer Science Research and Technology, 7(11),80-84.
[12] Zong, X. (2021). Regulatory Frameworks for Personal Information Protection in the Digital Era. Legality Vision, 16, 104–106.
[13] Solove, D. J. (2012). Introduction: Privacy Self-Management and the Consent Dilemma Symposium: Privacy and Technology. Harvard Law Review, 126(7), 1880–1903.
[14] Mansoor, M. (2021). Citizens' trust in government as a function of good governance and government agency's provision of quality information on social media during COVID-19. Government Information Quarterly, 38(4), 101597.
[15] Beshi, T. D., & Kaur, R. (2020). Public Trust in Local Government: Explaining the Role of Good Governance Practices. Public Organization Review, 20(2), 337–350.

ISSN 2616-7433 Vol. 7, Issue 4: 10-17, DOI: 10.25236/FSST.2025.070402

[16] Singh, S., & Kumar, R. (2024). SOCIAL CONTRACT THEORY AND IT'S DIMENSIONS- A CRITICAL REVIEW. NUJS Journal of Regulatory Studies, 9, 108-130.
[17] Talesh, S. A. (2018). Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses. Law & Social Inquiry, 43(02), 417–440.
[18] Taylor, N. (2002). State Surveillance and the Right to Privacy. Surveillance & Society, 1(1), 66–85.
[19] Chen, L. (2018). Algorithmic Recommendations Under the Panopticon Model: A Case Study of Toutiao. New Media Research, 04(07), 54–55.
[20] Yuan, D. (2010). The New Media Monitoring System From the Perspective of Foucault's Superpanopticon. Journal of China Three Gorges University (Humanities & Social Sciences), 32(S2), 187–188.
[21] Gu, L., & Wang, S. (2017). The Conflict Between Social Governance and Citizens' Privacy Rights: Public Video Surveillance from the Perspective of the Super Panopticon Theory. Modern Communication (Journal of Communication University of China), 39(06), 34–38.
[22] Xu, Y. (2021). "Intensification" and "Diffusion": The Panopticon in Social Media. Radio & TV Journal, 12, 190–192.
[23] Lu, A. (2017). A comparative study of the Super-Panopticon of Post and the Panopticon of Foucault Theory Research, Theory Research, 07, 105–106.
[24] Zhang, P. (2007). Analysis of Legal Protection of Personal Information in the Internet Age. Journal of Huaibei Normal University (Philosophy and Social Sciences), 01, 88–90.
[25] Dong, S., Zhang, L., & Zhou, Y. (2020). Telecom Fraud, Network Security and Government Accountability——A Case Study of XU Yu-yu. Journal of Luohe Vocational and Technical College, 19(04), 65–67.
[26] Wu, J., & Fang, X. (2024). Five years of GDPR enforcement in the EU: Achievements, Challenges, and Lessons Learned. Journal of Shanghai Jiaotong University (Philosophy and Social Sciences), 32(03), 82–99.