Proceedings of Business and Economic Studies, 2024, Volume 7, Issue 6
http://ojs.bbwpublisher.com/index.php/PBES
Online ISSN: 2209-265X
Print ISSN: 2209-2641

Legal Risks and Governance Strategies for Open Public Data in China

Linglan Xia*

Law School, Tianjin Normal University, Tianjin 300382, China

***Corresponding author:** Linglan Xia, xllxia777@163.com

Abstract: With advancements in information technology and the increasing demand for data-driven governance, the openness of public data has become essential for global governance and social innovation. However, legal risks related to privacy protection, data security, intellectual property, liability allocation, and legal adaptability pose significant challenges to data governance in China. This paper analyzes these risks and proposes three strategies: enhancing the legal framework through clear data classification and accountability mechanisms, establishing regulatory bodies to monitor data usage, and promoting public education on data privacy. These strategies aim to address gaps in legal discourse and guide effective data governance, contributing to the secure development of open data initiatives in China and beyond.

Keywords: Public data; Data openness; Legal risks; Governance strategies

Online publication: December 24, 2024

1. Introduction

The rapid advancements in information technology and the emergence of the big data era have rendered the openness of public data a critical issue in global governance. China's ongoing exploration and initiatives in this area reflect its substantial commitment to enhancing public data openness at the national level. The development of relevant legislation and policy frameworks has established a robust foundation for the effective management and utilization of public data.

China's data legislation is currently at a pivotal stage of development. Since the enactment of the Cybersecurity Law in 2017, the management of public data has increasingly been subjected to systematic legal regulation. The subsequent introduction of the Data Security Law and the Personal Information Protection Law in 2020 marked significant advancements in the rule of law governing data governance in China. These laws have established standards for data classification and usage while strengthening protections for personal privacy and data security. Nevertheless, existing legal frameworks exhibit limitations in their ability to adapt to the rapidly evolving technological landscape and the complexities of contemporary societal demands.

At the institutional level, government departments play a central role in advancing public data openness. Agencies such as the National Development and Reform Commission, the Cyberspace Administration of China, and local digital offices are responsible for integrating and disseminating public data. Their responsibilities include formulating policy frameworks, overseeing implementation, and facilitating data sharing and utilization, all of which aim to promote a collaborative approach to data governance.

In practice, the openness of public data has yielded encouraging results. Numerous local governments have established public data platforms spanning critical sectors such as transportation, healthcare, and education, thereby providing valuable data resources for both the public and enterprises. However, these initiatives face significant challenges, including inconsistencies in data quality, risks of privacy breaches, and inadequate regulatory oversight [1].

2. Major legal risks faced by public data openness in China

As China advances its public data openness initiatives, associated legal risks have become increasingly pronounced. These risks not only jeopardize the security and effective utilization of data but also threaten to erode public trust and disrupt social stability.

2.1. Privacy protection risks

Privacy protection risks constitute one of the most significant challenges in the realm of public data openness. As substantial volumes of personal data are collected and processed, the likelihood of information leakage has markedly increased. The Personal Information Protection Law mandates that the collection and processing of personal information adhere to the principles of legality, fairness, and necessity. However, during the data openness process, many institutions struggle to fully comply with these principles, leading to inadequate protection of personal information. Security vulnerabilities in data openness platforms, along with deficiencies in information-sharing mechanisms, make personal data susceptible to unauthorized access and misuse. This not only exposes individuals to potential economic losses but also threatens to erode public trust, thereby undermining the credibility of governments and related institutions.

2.2. Data security risks

Data security risks are primarily manifested in the storage, transmission, and utilization of data. As cyberattack techniques continue to advance, public data increasingly faces threats from hacking and misuse. In recent years, the frequency of data breaches has escalated, resulting in substantial volumes of public data falling into the hands of malicious actors. These attacks not only compromise the integrity and availability of data but also pose significant threats to social and national security. Existing security measures often fall short of effectively addressing complex cybersecurity challenges, particularly when managing large and diverse datasets [2]. Thus, it is imperative to establish a comprehensive data security management framework to enhance monitoring and protective measures for data.

2.3. Intellectual property risks

Intellectual property risks primarily arise from the ambiguous distinctions between public and commercial data, leading to significant legal disputes. As public data becomes increasingly accessible, businesses are leveraging this information for commercial purposes. However, the conflation of public and commercial data poses substantial risks of intellectual property infringement. For instance, commercial entities that utilize public data without proper authorization may inadvertently violate third-party intellectual property rights, resulting in legal conflicts. Furthermore, the openness of public data can adversely affect the market value of commercial data, thereby jeopardizing the economic interests of businesses. Therefore, it is essential to clearly delineate the boundaries between public and commercial data and to reinforce mechanisms for the protection of intellectual property rights.

2.4. Liability risks

Liability risks emerge from the ambiguity regarding the responsibilities of various stakeholders involved in data usage. The utilization of public data currently involves multiple parties, including government agencies, data providers, and data users. However, the rights and responsibilities of these entities are often inadequately defined in practice, complicating accountability in cases of data breaches, misuse, or other forms of misconduct. For instance, when a data user inflicts harm on another party through the use of public data, it is frequently unclear whether liability rests with the data provider, the data user, or the government agency, often due to the lack of clear legal standards. This uncertainty not only complicates the application of legal principles but also undermines the responsible management and utilization of data. Therefore, it is essential to establish a comprehensive legal framework that explicitly delineates the responsibilities of all parties involved in data usage.

2.5. Regulatory adaptability risks

Regulatory adaptability risks refer to the inadequacy of existing laws in effectively addressing the rapidly evolving technological landscape. As data technologies advance—particularly with the widespread implementation of artificial intelligence and big data analytics—current legal frameworks face unprecedented challenges [3]. For instance, regulations governing data collection, processing, and sharing often lag behind technological innovations, resulting in a significant disconnect between legal standards and technological realities. Furthermore, the emergence of new technologies may introduce novel legal dilemmas, such as algorithmic transparency and data ownership, which existing legislation has not sufficiently addressed. Therefore, to effectively navigate this dynamic environment, it is essential to expedite the adaptation and revision of legal regulations, ensuring that public data openness operates seamlessly within a comprehensive legal framework.

The legal risks associated with the openness of public data in China are both intricate and multifaceted, underscoring the urgent need for comprehensive legal research and innovative institutional frameworks. These initiatives are essential for safeguarding the healthy development of public data practices, facilitating the responsible utilization of data resources, and promoting overall societal advancement.

3. Governance strategies for addressing legal risks in China’s public data openness

In light of the legal risks associated with public data openness, it is essential for China to adopt effective governance strategies that facilitate the seamless advancement of data initiatives while safeguarding public interests. This section proposes three strategic approaches: enhancing legal frameworks, establishing robust data oversight mechanisms, and promoting comprehensive public education and engagement.

3.1. Enhancing the legislative framework

Revising and enhancing the existing legal framework is crucial to addressing the emerging challenges posed by public data openness. Although China has established a comprehensive set of laws governing data protection and management, these regulations often lag behind rapid technological advancements and the complexities of societal needs. A thorough evaluation of current legislation, followed by targeted revisions aligned with practical realities, is essential to improve the specificity and operability of these legal provisions [4].

3.1.1. Establishing clear data classification standards

Precise classification standards for public, personal, and commercial data are critical to clearly delineating the usage and protection requirements for each category. This clarity provides a robust legal foundation for lawful data utilization and reduces the potential for legal disputes arising from ambiguous definitions and overlapping boundaries. By defining these categories, stakeholders can navigate regulatory frameworks effectively, ensuring compliance and fostering a trustworthy data ecosystem [5].

3.1.2. Strengthening data usage regulations

To protect personal privacy and data security within the context of public data openness, the legal framework governing data collection, processing, and sharing must be strengthened. Laws should explicitly articulate the principles of legality, reasonableness, and necessity that underpin data usage, offering comprehensive guidelines for users. Enhanced regulations will ensure responsible and ethical data utilization, thereby fostering public trust and safeguarding individual rights.

3.1.3. Establishing accountability mechanisms

Well-defined accountability mechanisms are essential for enforcing stringent penalties against data breaches, misuse, and other violations. Such measures enhance legal awareness among data users and act as a significant deterrent to potential misconduct, safeguarding public interests. A culture of accountability reinforces the responsible use of data and bolsters public confidence in data governance practices.

3.2. Establishing data regulatory mechanisms

Specialized institutions dedicated to overseeing data usage and security are crucial for ensuring the transparency and integrity of public data access. Currently, government departments face overlapping functions and inadequate coordination in data management, which compromise regulatory efforts. A dedicated regulatory agency responsible for the integration, management, and supervision of public data would address these challenges by enhancing accountability, streamlining processes, and promoting a coherent approach to data governance.

3.2.1. Monitoring data usage

Regular monitoring of public data usage is vital for ensuring compliance with relevant laws and regulations. This process should include systematic audits and evaluations to identify and address potential issues promptly. A comprehensive monitoring framework enhances accountability among data users and fosters a culture of responsible data stewardship, reinforcing public trust in data governance.

3.2.2. Establishing data security standards

Unified data security standards and operational guidelines tailored to industry-specific requirements and technological advancements are essential. These standards should encompass all stages of data handling—storage, transmission, and processing—to ensure data integrity and security throughout its lifecycle. Robust security protocols can significantly mitigate vulnerabilities, enhance trustworthiness, and protect sensitive information, laying a foundation for responsible data management.

3.2.3. Enhancing transparency and accountability mechanisms

A transparent framework for data openness and usage is essential for ensuring public access to information about data utilization. Transparency fosters trust among stakeholders and encourages responsible data management practices. Robust accountability mechanisms should also hold institutions and individuals liable for violations of established standards, upholding the integrity of data governance and enhancing public confidence in the management of data resources.

3.3. Public education and participation

Enhancing public awareness of data privacy and security is essential for the sustainable development of open public data initiatives. An informed citizenry improves transparency and fosters active societal participation in data governance. By deepening understanding, individuals are more likely to support data openness and engage in governance processes, contributing to a responsible and collaborative data ecosystem.

3.3.1. Conducting public education initiatives

Educational outreach programs, including lectures, seminars, brochures, and online courses, are crucial for raising public awareness of personal data privacy and security. These initiatives inform individuals of their rights and provide strategies to mitigate privacy risks. By fostering an informed citizenry, such efforts elevate the culture of data protection and empower individuals to navigate data governance complexities effectively.

3.3.2. Promoting public participation in data governance

Establishing a public consultation platform is vital for incorporating diverse perspectives into data governance. Such a platform facilitates the collection and synthesis of public opinion, fostering trust in data management practices and encouraging active public engagement. This participatory approach supports the development of robust legal frameworks that promote the secure and transparent sharing of public data.

3.3.3. Enhancing transdisciplinary collaboration

Strategic alliances with academic institutions, research organizations, and industry bodies are essential for advancing research and practical initiatives focused on data privacy and security. Transdisciplinary partnerships integrate diverse perspectives, driving innovation and progress in public data governance.

The implementation of these strategies is pivotal in establishing a robust legal framework that supports the secure utilization and open dissemination of public data. These measures aim to mitigate legal risks significantly and lay a solid foundation for the sustainable development and societal advancement of public data practices.

4. Conclusion

The analysis has examined the legal risks associated with China's public data disclosure initiatives, focusing on privacy protection, data security, intellectual property rights, liability delineation, and regulatory adaptability. These risks present a dual challenge: hindering the effective utilization of public data and potentially eroding public trust in data openness policies. In response, three strategic governance measures have been proposed: strengthening legal frameworks, establishing robust data oversight mechanisms, and enhancing public education and engagement. These measures are critical for constructing a solid legal infrastructure for public data disclosure, ensuring its secure and compliant use.

Future research should prioritize several key areas. First, a comprehensive investigation into the influence of emerging technologies on public data disclosure is essential, with particular attention to how artificial intelligence and big data analytics are reshaping data collection and usage practices and the corresponding implications for the existing legal framework. Second, comparative international studies should be emphasized to derive insights from successful practices abroad that can enhance domestic legal frameworks in public data disclosure and legal risk management. Third, the interplay between personal privacy protection and data security in the context of international cooperation emerges as a pressing issue requiring immediate attention.

These research directions hold the potential to provide a robust theoretical foundation for the sustainable development of public data disclosure while offering practical guidance for policymaking and implementation.

Funding

Tianjin Education Commission Research Program in Humanities and Social Sciences (Project No. 2022SK064)

Disclosure statement

The author declares no conflict of interest.

References

[1] Ran L, Zhang X, 2020, Research on Data Security Policies in Local Government Data Openness. Journal of Information, 39(11): 96–103.

[2] Zhang X, Cao Q, 2023, Research on the Legal Mechanisms for the Confirmation and Authorization of Public Data. Comparative Law Studies, 2023(3): 41–55.

[3] Song S, 2023, Building a Mechanism for Public Data Openness Centered on Authorized Operations. Legal Science (Journal of Northwest University of Political Science and Law), 2023(1): 83–88.

[4] Gao F, 2023, The Data Holder Rights of Public Institutions: The Fundamental System of a Diverse Data Openness Framework. Administrative Law Studies, 2023(4): 91–102.

[5] Shen B, Li J, 2023, On the Typification Regulation of Public Data and Its Legislative Implementation. Journal of Wuhan University (Philosophy and Social Sciences Edition), 76(1): 67–77.