International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 4, Jul-Aug 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Research on Data Security Issues in Smart City Construction ---- The Path of Collaborative Governance of Law and Technology

He Rui Qi, Jian Song Yu, Nazila Ailiyeer, Zebanuer Tuerhong

Beijing Wuzi University, Beijing, China

ABSTRACT

Against the backdrop of the increasing popularity of global digitization, smart cities, as a new concept in urban development, are profoundly changing people's lifestyles and urban governance patterns. However, with the widespread application of projects such as Hangzhou's "City Brain" and Shenzhen's intelligent transportation, data security has become a concern. Our research focuses on potential legal or technical vulnerabilities in data collection, sharing, supervision, and other links during smart city construction. Through literature research, case analysis, and other methods, we analyze the current data security issues. The study finds that the "Personal Information Protection Law" cannot effectively play its role in smart city scenarios. There are sometimes misunderstandings in data sharing between departments, and the responsibilities of various subjects are unclear in division of labor. Therefore, our research proposes solutions from three aspects: improving laws and regulations, unifying technical standards, and innovating supervision mechanisms, to better balance technological development and protection of individual rights.

KEYWORDS: *Smart City; Data Security; Personal Information Protection; Legal Regulation; Regulatory Coordination.*

How to cite this paper: He Rui Qi | Jian Song Yu | Nazila Ailiyeer | Zebanuer Tuerhong "Research on Data Security Issues in Smart City Construction ---- The Path of Collaborative Governance of Law and Technology" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-4, August 2025, pp.805-808, URL: www.ijtsrd.com/papers/ijtsrd97322.pdf

IJTSRD97322

I. INTRODUCTION

A. Research Background

Nowadays, more than 500 cities in China have launched smart city construction projects. From the real-time traffic monitoring system of Hangzhou's "City Brain" [1] to the travel data collection of Shenzhen's 扫码 (scan code) subway, various smart applications generate a huge amount of data every day. However, data security incidents often occur. Cases such as the leakage of a certain city's star nucleic acid test records and the reselling of customer information by courier company employees all indicate that there are major loopholes in smart city data management. Although the "Personal Information Protection Law" has been promulgated and implemented, it cannot be well applied in specific scenarios like smart cities, failing to exert its effectiveness, leading to the law lagging behind technological development.

B. Research Significance

From a practical perspective, our research aims to solve the difficulties faced by ordinary people in protecting their data security, whether enterprises are compliant when participating in smart city projects and whether there are risks of data security leakage, and whether the government can balance the development of smart cities and data security, as well as the protection of privacy. It provides some references for the government to formulate data security-related policies. Theoretically, our research intends to provide new research perspectives and viewpoints in this field.

C. Research Innovations

Our research aims to combine legal and technical aspects, focusing on breaking through three innovative directions: First, conduct in-depth research on how data collection and processing are authorized, and propose a detailed legal review system for issues such as the placement of intelligent devices exceeding necessary limits and the lack of anonymization technical standards. Second, focus on optimizing the norms for data sharing and utilization, and strive to

solve the problem of unclear division of responsibilities in data sharing between departments and subjects. Third, find new ways to clarify the responsibilities for data protection and ensure that those in charge cooperate well. For example, it is necessary to clearly define what the government, companies, and computer technicians should do, so that no one can shirk their responsibilities. In addition, different departments should also cooperate with each other to manage data well and prevent problems.

II. Current Situation and Problems of Smart City Data Security

A. Defects in the Authorization Mechanism for Data Collection and Processing

In smart city construction, there are obvious deficiencies in the authorization of data collection links [2]. Taking face recognition cameras as an example, grass-roots units such as neighborhood offices often do not know how to check the appropriateness and legality of installing such monitoring equipment. As a result, the number of devices is excessive. For example, a community with only over 1,000 households has installed more than 300 cameras, disturbing residents' private lives. In addition, the current technology called "anonymization", which aims to hide personal information in data, has no clear standards to regulate how to truly hide it. Some data claimed to be "anonymous" can actually be identified with technical means. For instance, a research institution obtained public medical data that was said to be anonymous, and combined it with other publicly available information, 居然 identified the real identities of more than 80% of patients. As a result, the attempt to protect everyone's privacy failed.

B. Lack of Norms for Data Sharing and Utilization

Although there are policies encouraging data sharing to break information silos, there is no unified set of rules in practice. For example, when government departments and companies want to exchange data, they often get stuck due to issues such as unclear responsibilities and benefits. In one city, the transportation department wanted to cooperate with an internet company to develop an intelligent parking system, but the project was delayed for half a year because of unclear ownership and usage scope of the data. Moreover, there are no unified standards for processing sensitive information to remove privacy during data sharing. Different departments have different understandings and practices of "desensitization". For example, a medical data sharing platform had loose standards for handling sensitive information, leading to the connection of patients' names and their diseases, which caused a bad social impact.

C. Insufficient Data Security Responsibility and Regulatory Coordination

In smart city construction, there are many participants such as the government, companies, and technology manufacturers, but current legal regulations do not clearly define their respective responsibilities. In case of data leakage, it is unclear which party among platform companies, technology manufacturers, and government departments should be held responsible, making it difficult to pursue accountability. For example, when user information was leaked from an e-commerce platform, the platform blamed the technology manufacturer for system vulnerabilities, while the technology manufacturer claimed that the platform failed to manage security. In the end, it was unclear who was responsible, leading to more disputes. In addition, different departments have not formed a good cooperative supervision method, and each department has different management standards, resulting in low efficiency. Departments such as market supervision, cyberspace administration, and public security may have overlapping or vacant supervision in data security. If three departments file cases to investigate the same data security incident, it will waste management resources.

III. Research Methods and Processes

A. Literature Research Method

First, we collected domestic and foreign papers and research reports on data security in smart cities from CNKI and Web of Science. Then, these materials were centralized, processed, and classified to clarify the existing knowledge, current research focuses, and latest research directions in this field. In addition, we found policies, regulations, and standards related to smart city construction and data security management issued by national and local governments from government websites. Through careful analysis of these regulations, we understood what policies encourage and what laws require, which laid a solid foundation for our research.

B. Questionnaire Survey Method

Targeted questionnaires were designed for different groups such as government departments, enterprises, and citizens. The questionnaire content covers cognition, attitude, risk perception, etc., towards smart city data security [3]. During the survey, we used both online platforms and offline interviews, including people from government departments, companies, and ordinary citizens. In this way, opinions from different groups were collected, representing more people's ideas.

C. Case Analysis Method

We selected more than 20 typical cases of data security in domestic and foreign smart city construction, including both successful experiences and lessons. For example, when the health code information was leaked in one place, we carefully examined how it started, the process, the impact, and the subsequent handling. We found many problems, such as non-compliant consent collection, casual information sharing procedures, and unclear responsible parties, which led to the incident. In addition, we also studied foreign situations, such as the EU's good practices in smart city data security management. Then, we summarized effective methods and models for data security protection in different situations, and drew universal inspirations and solutions from these real cases.

IV. Solutions to Smart City Data Security

A. Improve the Legal Authorization Mechanism for Data Collection and Processing

1. Refine Authorization Scope and Procedures

Formulate the "Measures for the Administration of Smart City Data Collection" as a universal rule. The measures will stipulate that the installation of intelligent devices must have necessary reasons and cannot be done arbitrarily. For example, grass-roots units like neighborhood offices that want to install devices collecting sensitive information such as face recognition must report to the county or municipal cyberspace administration and obtain approval. Moreover, during the application, details such as the number of devices, installation locations, reasons for data collection, and storage duration must be made known to the approving department. Establish a negative list system based on the "minimum necessary" collection principle to prohibit the collection of personal information unrelated to smart city services [4].

2. Unify Anonymization Technical Standards

The state will let the special standard-setting committee take the lead in formulating the "Technical Specifications for Smart City Data Anonymization" to set detailed rules for data anonymization. These rules will specify the technical parameters for anonymizing data and how to judge the effectiveness of anonymization. For example, if anonymized data can still be identified, the responsible party must bear corresponding responsibilities.

B. Optimize the Norm System for Data Sharing and Utilization

1. Establish a Cross-Departmental Data Sharing Legal Framework

Promote the formulation of the "Regulations on the Administration of Government Data Sharing" to set clear rules for data sharing between government departments. The regulations will clarify the responsibilities, rights, procedures, and safety requirements of different government departments in data sharing. In addition, a cross-departmental data sharing coordination team will be established to list sharable data and mediate disputes between departments during data sharing. At the same time, an accountability mechanism will be established. If data is leaked during sharing, the relevant departments and personnel will be held responsible in accordance with the rules.

2. Unify Data Desensitization Standards

Formulate the "Guidelines for Smart City Data Desensitization" to clarify how to protect confidential information in data. The guidelines will classify data according to sensitivity levels, with different processing methods and standards for each level. For example, highly private information such as names and ID numbers should be encrypted with irreversible methods; semi-private information such as addresses and phone numbers can be partially hidden (e.g., only showing the middle digits of phone numbers). In addition, a mechanism to inspect data protection will be established to regularly check whether data sharing platforms handle data in accordance with the rules, ensuring information security.

C. Innovate Data Security Responsibility and Regulatory Coordination Mechanisms

1. Clarify the Responsibility Boundaries of Multiple Subjects

In the implementation rules of the "Personal Information Protection Law", the responsibilities of different participants in smart cities, such as the government, enterprises, and technology providers, must be clearly defined. If the government leads a smart city project, it shall bear the main responsibility for data security. Enterprises shall bear direct responsibility for the services and data they provide. For example, a company developing a smart city life service APP that collects a lot of user information must ensure the security of this information and prevent leakage. Technology providers are also responsible for ensuring the security of their technical products and services. In addition, a reverse accountability mechanism must be established. In case of data leakage, a "double investigation" shall be conducted: on the one hand, investigate the person directly responsible for the leakage; on the other hand, investigate the management responsibility to see if leaders failed to manage well, formulate safety rules, or supervise effectively. This way, everyone will take data security in smart cities seriously and better protect our personal information.

2. Build a Cross-Departmental Collaborative Regulatory Model

We will establish a "National Smart City Data Security Supervision Committee" involving personnel from departments such as cyberspace administration, public security, market supervision, and industry and information technology to jointly inspect and handle data security issues. At the same time, unified supervision standards and procedures will be formulated to ensure consistent practices and share supervision resources and information for more convenient work. In addition, a "credit file" for smart city data security will be established to record the performance of enterprises and individuals in data security. Those who violate the rules and lose credibility will be jointly punished to prevent future violations.

V. Conclusions and Prospects

A. Research Conclusions

After carefully studying data security issues in smart cities, we found the following: Smart city construction is currently facing many data security challenges, such as undefined data usage rules, incomplete data sharing rules, and insufficient coordination among different departments in data security supervision. These problems arise because relevant regulations are updated slowly and cannot keep up with technological development, the responsibilities of many participants are unclear, and there is no perfect cooperation mechanism between different departments. However, we have also come up with some solutions, such as improving data usage rules, optimizing data sharing systems, and innovating collaborative supervision methods among departments.

B. Research Prospects

Future research can be deepened in the following aspects:

The first direction is to study how technology and regulations can cooperate well. For example, how new technologies such as blockchain and privacy computing can be applied to data security protection in smart cities, while formulating relevant rules to ensure appropriate application of technology.

The second direction is to learn from other countries and regions' experiences in managing smart city data security, drawing on their successful practices and learning from their mistakes to improve our work.

The third direction is to pay attention to new issues brought by emerging technologies. For example, 5G, the Internet of Things, and artificial intelligence may bring new data security risks, and measures must be taken to address these risks.

References

[1] "Construction Background and Core Applications of City Brain Empowering Urban Public Security"

[2] "Discussion on Countermeasures for Smart City Construction in Xigang District, Dalian"

[3] "Research on Risk Management of China's Express Payment Methods"

[4] "Research on Legal Issues of Financial Privacy Protection in Internet Credit Reporting"