Journal of Commercial Law Review
2025, VOL. 9, NO. 3, 45-47
DOI: 10.47297/wspjclrWSP2516-249709.20250903

A Study on the Legal Regulation of Artificial Intelligence and Big Data Crimes in the Context of Smart Cities

Yanhao Liang

Beijing Dongwei Law Firm, Beijing, 100027, China

ABSTRACT
In the construction of smart cities, while artificial intelligence and big data technologies improve governance effectiveness, they also give rise to new crimes such as data leaks, algorithmic discrimination, and system attacks, posing challenges to residents' rights and urban security. Current laws and governance mechanisms lag behind, with unclear responsibility determination and insufficient regulatory measures becoming prominent. Drawing on the smart city technology ecosystem, this article analyzes the types and characteristics of these crimes and the challenges in addressing them. Drawing on domestic and international experience, it proposes regulatory approaches from the perspectives of legislation, judicial practice, ethics, and multi-faceted governance, providing theoretical and practical guidance for achieving the safe and sustainable development of smart cities.

KEYWORDS
Smart city; Artificial intelligence crime; Big data crime; Legal regulation; Governance effectiveness

1 Introduction

Driven by the wave of digitalization, smart cities have become a core direction of urban development worldwide. By integrating artificial intelligence algorithms, IoT sensing devices, and massive data analysis technologies, smart cities have achieved intelligent upgrades in areas such as traffic scheduling, energy distribution, and public services, significantly improving urban operational efficiency and residents' quality of life. However, technological empowerment harbours multiple risks [1]. In 2023, a data platform vulnerability in a smart community led to the leakage of private information of 100, 000 users. In 2024, a city's intelligent transportation system was attacked by a malicious algorithm, causing widespread congestion. The autonomous decision-making capabilities of artificial intelligence blur the boundaries of responsibility for traditional crimes, and the centralized storage of big data amplifies the harmful consequences of data misuse. However, the current legal system still lags behind in regulating new types of technological crimes. This article focuses on the unique technological ecosystem of smart cities and examines AI and big data crimes within the macro framework of urban governance. It analyzes both the technical mechanisms of crime and institutional governance countermeasures, aiming to achieve a healthy balance between "technological progress" and "legal order."

2 Types and characteristics of big data crimes in smart cities

2.1 Diverse types of crime

First, there is data misuse crime. This manifests itself as the unauthorized collection, trading, or tampering of city operational data, including sensitive information such as residents' biometrics, travel history, and consumption records. For example, some companies exploit the privileges of smart medical systems to illegally obtain patient medical records for commercial purposes, or steal household lifestyle data through IoT devices such as smart water and electricity meters [2]. The core characteristic of this type of crime is the separation of data ownership and usage rights. The hidden nature of data transfer makes tracing the source extremely difficult. Secondly, algorithmic manipulation crimes leverage artificial intelligence algorithms to implement discriminatory decisions or malicious manipulation. For example, smart employment platforms use algorithmic models to create hidden employment barriers for specific groups, and smart financial systems leverage big data analysis to carry out targeted fraud. The "black box" nature of algorithms makes criminal behavior more covert, and their large-scale application could lead to systemic social injustice [3]. Finally, systemic attack crimes target the intelligent systems of critical smart city infrastructure, including tampering with smart grid scheduling algorithms to cause regional power outages and hacking into smart security systems to create security vulnerabilities.

2.2 Peculiar criminal characteristics

Compared to traditional crimes, AI and big data crimes in smart city environments exhibit three new characteristics: First, the diversity of perpetrators. Perpetrators can include technology developers, platform operators, external hackers, or even the AI system itself (such as autonomously evolving malicious algorithms), significantly increasing the difficulty of assigning responsibility. Second, the radiative nature of the harm. The interconnectedness of data allows the impact of

crime to transcend physical space. A data analysis vulnerability in a single community could jeopardize the emergency response system of an entire city. Third, technology dependence [4]. The commission of these crimes relies heavily on specialized knowledge. For example, exploiting vulnerabilities in federated learning algorithms to poison data requires mastery of both machine learning and cybersecurity technologies.

3 The real dilemma of smart city crime governance

3.1 Data privacy protection

In the construction of smart cities, a vast amount of personal data is collected and utilized, including identity information, travel history, and consumption habits. Leakage or misuse of this data would seriously infringe upon residents' privacy rights. Some companies, driven by commercial interests, excessively collect data without effective security measures. The flow of data between multiple entities also increases the risk of leakage. How to protect residents' data privacy while leveraging data to improve city services has become an urgent ethical dilemma.

3.2 Issues of fairness and justice

The application of smart city technologies may exacerbate social inequalities. For example, if intelligent decision-making systems are trained based on biased data, they may produce discriminatory outcomes in the allocation of educational resources and employment opportunities, further disadvantage disadvantaged groups [5]. Furthermore, differences in the ability of different groups to access and use smart city technologies have led to a "digital divide," further impacting the realization of social fairness and justice.

4 Comparison and reference of international and domestic governance experiences

4.1 Typical international models

The EU's Digital Services Directive framework requires smart city platforms to establish a "data impact assessment mechanism" and implement mandatory audits for high-risk algorithm applications; it also clarifies the "security obligations" of platform operators and implements a "72-hour mandatory reporting" system for data breaches. Singapore's "Smart Nation Blueprint" governance model establishes a cross-departmental "Data Governance Committee," develops a "Public Data Sharing Framework," and strictly distinguishes between government and corporate data access rights; it also implements an "Algorithm Accountability Labeling System," requiring public-facing intelligent systems to disclose their decision-making logic.

4.2 Exploration of domestic practices

Local legislation takes the lead. The "Shenzhen Special Economic Zone Data Regulations" for the first time clearly define the "safe use boundaries of public data" and stipulate that sensitive data in areas such as smart transportation and healthcare must utilize technologies such as "federated learning" to achieve "data availability without visibility." Industry self-regulation and innovation [6]. The Internet Society of China issued the "Smart City Data Security Self-Discipline Convention," encouraging companies to establish a "Data Security Officer" system and conduct "full lifecycle security assessments" of artificial intelligence systems.

5 Comparative analysis of ethical and legal case studies

By selecting typical smart city projects at home and abroad and comparing data from dimensions such as ethical dispute resolution and legal regulatory effectiveness, we can clearly demonstrate the practical differences between different governance models.

Table 1 Comparison of ethical dispute resolution efficiency in smart cities at home and abroad

Case Study Locations	Dispute Type	Time from dispute occurrence to response (d)	Problem solving cycle (d)	Public satisfaction (%)	Third-party involvement rate (%)
City A, China	Excessive Data Collection	15	68	52	10
City B, China	Algorithmic Discrimination	21	83	41	5
Country C, EU	Excessive Data Collection	7	32	78	100
City D, US	Algorithmic Discrimination	5	25	82	90

Data Source: This article researches and compiles typical cases both domestically and internationally. For EU and US cases, reference is made to reports related to the Digital Services Directive and the US ICMA white paper. For Chinese cases, reference is made to research and public records in first-tier cities in China.

As shown in Table 1, domestic cases lag significantly behind in dispute response speed and resolution efficiency, with

public satisfaction rates below 50% and an extremely low rate of third-party involvement. In contrast, European and American cases have an average response time of only 6 days, a resolution cycle of approximately 28 days, a satisfaction rate exceeding 75%, and a third-party involvement rate generally exceeding 90%. This difference reflects the advantages of mature multi-faceted governance mechanisms abroad.

Table 2 Comparison of the effectiveness of smart city legal regulation in china and abroad

Case Study Regions	Number of relevant regulations (n)	Cost of illegal activities (10,000 yuan)	Proportion of compliant enterprises (%)	Repeat offense rate (%)	Success rate of residents' rights relief (%)
China	8	5-50	63	28	35
EU	12	100-2000	91	7	89
United States	15	80-1500	87	11	82

Data source: China's data comes from the evaluation of the "Shenzhen Special Economic Zone Data Regulations" and other sources; EU data comes from the DSA implementation report and other sources; US data refers to the FTC regulatory report and Department of Justice statistics.

Table 2 shows that China has relatively few smart city regulations and a relatively low cost of violations. This results in only 63% of companies being compliant, a 28% repeat violation rate, and a less than 40% success rate for residents seeking redress [7]. The EU, through a well-developed regulatory system and high violation costs, has achieved a 91% corporate compliance rate and an 89% success rate for redress, providing an important reference for my country.

6 Conclusion

The governance of AI and big data crimes in smart cities requires a new system adapted to technological development. Currently, challenges include insufficient legal adaptation, unclear division of responsibilities, and weak ethical constraints. Solutions should include: legislation to fill regulatory gaps, judicial innovation in responsibility determination mechanisms, strengthening industry self-regulation and public oversight, and forming a multi-dimensional governance framework encompassing "law, ethics, technology, and the public." By balancing innovation and prevention through multi-stakeholder collaboration, we can overcome security challenges and achieve the healthy development of smart cities.

About the Author

Yanhao Liang, Male, Senior Partner, Deputy Director of the Criminal Law Committee, Master of Law in Criminal Law, Research Focus: Corporate Compliance Systems, Legal Risk Governance, and Criminal Defense Practice.

References

[1] O'Malley P., & Smith G. J. (2022). 'Smart'crime prevention? Digitization and racialized crime control in a Smart City. Theoretical Criminology, 26 (1), 40-56.

[2] Tutak M., & Brodny J. (2023). A smart city is a safe city: analysis and evaluation of the state of crime and safety in Polish cities. Smart Cities, 6(6), 3359-3392.

[3] Christofi A., Wauters E., & Valcke P. (2021). Smart Cities, Data Protection and the Public Interest Conundrum: What Legal Basis for Smart City Processing?. European Journal of Law and Technology, 12(1), 1-36.

[4] Kabir M. S., & Alam M. N. (2023). IoT, big data and Ai applications in the law enforcement and legal system: a review. International Research Journal of Engineering and Technology (IRJET), 10(05), 1777-1789.

[5] Oatley G. C. (2022). Themes in data mining, big data, and crime analytics. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 12(2), e1432.

[6] Butt U. M., Letchmunan S., Hassan F. H., Ali M., Baqir A., Koh T. W., & Sherazi H. H. R. (2021). Spatio-temporal crime predictions by leveraging artificial intelligence for citizens security in smart cities. IEEE Access, 9, 47516-47529.

[7] Palanivinayagam A., Gopal S. S., Bhattacharya S., Anumbe N., Ibeke E., & Biamba C. (2021). An optimized machine learning and big data approach to crime detection. Wireless Communications and Mobile Computing, 2021(1), 5291528.