The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Navigating the Labyrinth: The Legal Framework for Smart Cities in India

- By Gaurab Das

ABSTRACT

The Smart Cities Mission (SCM) of the Government of India launched ipagen 2015 is the globe's most ambitious initiative for creating smart cities. It seeks to revamp 100 of the nation's cities into eco-friendly, citizen-driven, and economically sustainable urban agglomerations with technology- and data-facilitated governance. But the fast-tracked digitization and infrastructure transformation integrated into the new model of a creative city carry extensive legal implications that cannot be addressed through India's existing jurisprudence. This article offers a critical and holistic examination of the main legal concerns generated by India's Smart City mission. It examines the gigantry of loopholes in law, with particular focus on four prominent themes: data privacy and protection, cybersecurity, intellectual property rights, and accountability for algorithmic decision-making. The case is that while the SCM envisions a future for technology, it does so in the absence of regulation, posing risks to human rights, public accountability, and fair urban development. The study relies on an examination of recent Indian legislation, such as the Information Technology Act, 2000, the newly enacted Digital Personal Data Protection Act, 2023, and the relevant constitutional provisions. The article sums up by suggesting a hybrid model of governance that includes robust rights-oriented legislation and adaptive regulatory bodies, making India's smart cities not only technologically advanced but legally secure, socially just, and constitutionally harmonized.

Keywords: Smart Cities, India, Data Privacy, Cybersecurity, Intellectual Property, Algorithmic Governance, Digital Personal Data Protection Act, 2023, Legal Framework, Urban Law.

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

INTRODUCTION

Urbanization is one of the characteristic hallmarks of the 21st century. By 2050, over 50% of India's population will live in urban centers, putting the existing infrastructure, resources, and government under an unprecedented strain (Ministry of Housing and Urban Affairs [MoHUA], 2021). To meet this challenge, the Government of India initiated the flagship Smart Cities Mission (SCM) on 25 June 2015. The mission aims at "promote cities that provide core infrastructure and give a decent quality of life to its citizens, a clean and sustainable environment and application of 'Smart' Solutions" (MoHUA, 2015, p. 5). At the heart of this "smartness" is the integration of Information and Communication Technologies (ICT) into urban governance, forming a huge network of sensors, cameras, and data analysis software to maximize everything from traffic and garbage collection to electricity delivery and public safety.

While smart city technology's promise is alluring, its regulatory and legal basis to make them possible is still in its infancy and disjointed. The creation of a "digital twin" of a real city creates vast volumes of data, raises fundamental issues of surveillance and privacy, introduces new susceptibilities to cyber-attacks, and creates complicated issues with liability and intellectual property rights. As aptly explained by Green (2019), "The smart city is not just a technical project; it is a legal and political one, reconfiguring power, citizenship, and the public sphere" (p. 45).

This article contends that the existing law in India is not strong enough to tackle the various challenges of smart cities. The existing laws, which were formulated for the pre-digital era, are being retrofit to deal with digital realities, and the result is large gaps and inconsistencies. The recent enactment of the Digital Personal Data Protection Act (DPDPA) in 2023 is a welcome move, but it cannot in itself touch the broader legal environment. This study shall try to tackle such issues in a systematic manner. It will initially outline the conceptual and operational structure of Indian smart cities. It will proceed to put four areas of law to critical scrutiny:

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

1. Data Protection and Privacy: Analyzing the adequacy of the DPDPA, 2023, against the backdrop of mass urban data harvesting and the dangers of function creep and excessive surveillance.

2. Cybersecurity and Critical Infrastructure: Investigating the risks of networked urban systems and the sufficiency of current cybersecurity legal framework.

3. Intellectual Property Rights (IPR): Unraveling the complicated issues of ownership and licensing of data and algorithms produced by public-private collaborations.

4. Liability and Accountability: Resolving the "black box" problem of algorithmic decision-making and liability for harm resulting from autonomous systems.

With this critique, the paper aims to add its input to the debate on city governance in the digital age and propose an innovative legal framework that can place India's smart cities on the pillars of justice, equity, and accountability.

INDIAN SMART CITY: GOVERNANCE AND MODEL

The Indian definition of a smart city as conceived under SCM is not a strict definition but a "place-based" one. It is unequivocally mentioned in the mission document that there is "no one way of defining a smart city" (MoHUA, 2015, p. 7). The strategy is area-based development—retrofitting, redevelopment, and greenfield developments—and pan-city projects that use innovative solutions for the existing city-wide infrastructure.

The main institutional vehicle to execute the SCM in all the cities is the Special Purpose Vehicle (SPV). The SPV is a limited company formed under the Companies Act, 2013. Equity shares in the SPV are held equally by the state and urban local body (ULB). The SPV will be responsible for planning, appraisal, approval, financing, implementing, managing, operating, monitoring, and evaluation of the innovative city projects (MoHUA, 2015). This corporate form is intended to introduce efficiency, financial independence, and managerial adaptability, circumventing the classic bureaucratic hindrances of municipal government.

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

But this same model raises legal problems of its own. The SPV is floated at arm's length to the democratically elected ULBs, and this raises some very basic issues of democratic accountability and public participation (Bhattacharya & Rathi, 2015). When a private ICT provider enters into an agreement with an SPV to govern a city's data, the chain of accountability becomes muddled among the citizen, the elected member, the SPV, and the private firm. This public-private hybrid model of governance is rich terrain for court cases on matters of transparency, right to information, and the coercive enforcement of constitutional ideals upon a corporate body engaged in sovereign functions.

CRITICAL LEGAL CHALLENGES AND POLICY FAILURES

PRIVACY AND DATA PROTECTION

Data is the lifeblood of a smart city. An incessant stream of information is generated by Internet of Things (IoT) sensors, smart meters, GPS trackers, CCTV cameras, and citizen apps. It encompasses very intimate personal details, including location histories, travel patterns, power usage patterns, health data, and even social relationships. The gathering and handling of the data on that unprecedented scale endangers the fundamental right of privacy in its most elementary form for the first time, which the Supreme Court of India categorically held to be a fundamental right under Article 21 of the Constitution in its milestone verdict of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017).

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: AN INCOMPLETE PANACEA

The application of the DPDPA in 2023 marks a significant shift in Indian privacy legislation. It sets foundation principles, such as lawful purpose, data minimization, and storage limitation, and provides some data principals (individuals) with rights. Its operation in the context of a smart city, however, is filled with issues.

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

•Legitimacy of Purpose and Mass Surveillance: Reasons for gathering information in innovative city initiatives are typically framed in the general provision of "public interest" or "functions of the State," valid purposes under the DPDPA, 2023. However, public service and mass surveillance stand on a skinny line. For instance, a facial recognition grid of cameras (FRT) deployed for security in a smart city can easily become an all-pervasive surveillance machine, suppressing free assembly and speech (Suresh, 2021). The DPDPA, 2023, is not sufficiently equipped to prevent such "function creep," where data gathered for one purpose is channeled into another without explicit consent.

• Illusion of Consent: Notice-and-consent, the defining feature of most data protection systems, is no longer possible in the smart city. A citizen cannot reasonably deny consent to data collection that pertains to accessing basic city services, such as water, electricity, or public transportation, without jeopardizing their access to these services. This creates a coercive space in which "consent" is not freely given, but rather something required for inclusion in urban society (Sharma & Khanna, 2022).

• Exemptions to the State: The DPDPA, 2023, provides a general exemption to the government for processing personal data for purposes such as national security, research, and any "fair and reasonable" notified purpose. These general exemptions are available for use to circumvent key data protection principles essential for the functioning of smart cities, which could compromise the very rights this Act is meant to safeguard.

The European Union General Data Protection Regulation (GDPR) case law focuses on "data protection by design and by default." There is no Indian legislation mandating smart city programs to incorporate such principles as an integral part of their architectural design from the conceptual stage.

CYBERSECURITY OF CRITICAL URBAN INFRASTRUCTURE

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Smart cities congregate Operational Technology (OT) the infrastructure that controls physical processes, i.e., water supply, power supply, and traffic lights—along with Information Technology (IT). This integration radically increases the attack surface for malicious actors. This kind of cyber-attack on a smart city is not just a data breach anymore but also an imminent threat to national security and public safety. An attacker, for instance, is able to destroy a city's electricity grid, control water treatment chemicals, or jam traffic in bulk (Graham & Mann, 2018).

The key Indian legal framework for cybersecurity is the Information Technology Act, 2000, and assisted by the National Cyber Security Policy, 2013.

• Shortcoming of the IT Act, 2000: The IT Act is primarily dedicated to data protection crimes and e-commerce. It is not geared towards protection for sophisticated, interdependent cyber-physical systems that form city critical infrastructure. Though Section 70B sets up the Indian Computer Emergency Response Team (CERT-In), its powers and role are undermined if obligated to protect a complete urban system.

• No Critical Infrastructure Protection Act: India does not have a specific law for the identification and protection of Critical Information Infrastructure (CII). Though the National Critical Information Infrastructure Protection Centre (NCIIPC) has been set up, its power is limited to certain sectors, i.e., energy, banking, and transport. The term CII must be interpreted widely to encompass the integrated management systems of a smart city. Smart cities, with no industry-specific security requirements and stringent audit standards, are extremely vulnerable.

INTELLECTUAL PROPERTY RIGHTS (IPR)

The development and operation of smart cities rely heavily on collaborations between public SPVs and private technology firms. These partnerships generate valuable intellectual property, including the software platforms, data analytics algorithms, and, most importantly, the aggregated and anonymized datasets themselves.

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

- **Ownership of Data:** A fundamental legal question is: Who owns the data generated by a smart city? Is it the citizen who is the source of the data, the SPV (as the public authority), or the private company that designed the sensors and analytics platform? The DPDPA, 2023, vests the rights in the data principal, but it is silent on the ownership of anonymized or aggregated datasets, which have immense commercial value. Clear contractual agreements between SPVs and private partners are essential, but a lack of standardized models and bargaining power asymmetry often leads to public data being effectively privatized (Kitchin, 2014).
- **Ownership of Algorithms and Software:** The algorithms that power predictive policing, optimize traffic signals, or allocate resources are often developed by private entities. If a city SPV pays for the development, should the IPR reside with the city, or should the vendor retain it under a licensing agreement? If the vendor retains the IPR, the city may face vendor lock-in, exorbitant licensing fees, and an inability to audit or modify the "black box" algorithms that are making consequential public decisions. This contradicts the principles of transparency and accountability in public administration.

The current legal framework, primarily the Copyright Act, 1957, and the Patents Act, 1970, is not tailored to address these unique collaborative models of urban innovation, which may potentially stifle competition and undermine public control over essential urban governance tools.

LIABILITY AND ALGORITHMIC ACCOUNTABILITY

Smart cities increasingly deploy algorithms and Artificial Intelligence (AI) for automated decision-making. These systems are used for tasks ranging from detecting traffic violations automatically to allocating social welfare benefits and predicting crime "hotspots."

- **The "Black Box" Problem:** Many advanced AI and machine learning models are opaque, meaning it is difficult or impossible to understand how they arrived at a

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

particular decision. If an autonomous traffic management system erroneously issues a thousand fines, or a predictive policing algorithm disproportionately targets a minority community, who is liable? The principles of administrative law require that state action must be reasoned and non-arbitrary (State of West Bengal v. Anwar Ali Sarkar, 1952). An algorithmic decision that cannot be explained violates this fundamental principle.

- **Gaps in Tort Law:** Indian tort law, based on negligence and strict liability, struggles to accommodate harm caused by autonomous systems. Establishing a duty of care, breach, and causation is complex when the "wrongdoer" is a self-learning algorithm whose logic may be inscrutable even to its creators. There is a pressing need for a sui generis legal framework for AI liability, similar to the EU's proposed AI Liability Directive, which could include concepts like a "rebuttable presumption of causality" in cases involving high-risk AI systems.
- **Accountability Deficit:** The corporate structure of the SPV and the use of proprietary algorithms create an "accountability vacuum." The elected municipal council can deflect responsibility to the SPV, which in turn can blame the algorithm or the private vendor. This breaks the chain of direct accountability that is essential in a democratic setup, leaving citizens without an effective remedy for grievances arising from automated decisions.
- Liability in an Integrated Ecosystem: In case of a cascaded cyber-attack leading to physical destruction or loss of life, how the liability would be distributed is a lawyer's nightmare. Would it be the SPV, the municipal corporation, the tech provider whose software had a bug, or the third-party integrator? The present law of tort and the IT Act have no ready answers for such a situation with multiple stakeholders in a public-private partnership model.

THE WAY FORWARD: PROPOSALS FOR A ROBUST LEGAL ARCHITECTURE

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

To bridge the identified regulatory gaps, a multi-pronged legal and policy approach is necessary. Merely tinkering with existing laws will not suffice; a proactive and holistic governance model must be established.

1. **Enacting a Smart City Governance Act:** A dedicated national-level framework law is needed to provide a coherent structure for all innovative city projects. This Act should:
    - Mandate the creation of a **Data Governance Framework** for each smart city, requiring Data Protection Impact Assessments (DPIAs) for all new projects and enforcing privacy-by-design principles.
    - Clarify the **accountability relationship** between the SPV, the ULB, and the state government, ensuring that the SPV remains ultimately answerable to the elected council.
    - Establish mandatory **cybersecurity audits and standards** for all critical urban infrastructure, with clear reporting protocols to CERT-In and NCIIPC.
2. **Strengthening the DPDPA through Robust Rules:** The implementation of the DPDPA, 2023, will depend heavily on the rules framed by the government. These rules should:
    - Provide specific guidance on applying the law to smart city contexts, particularly limiting the use of facial recognition and other intrusive surveillance technologies.
    - Clarify the ownership and governance models for non-personal and anonymized data, ensuring that such public assets are governed for the public benefit.

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

3. **Developing Model Contracts and IPR Guidelines:** The MoHUA, in consultation with legal experts, should develop model contract frameworks for SPV-private partner agreements. These must be clearly defined:
    - IPR ownership, favoring models where the SPV retains ownership or has perpetual, royalty-free licenses to core software and algorithms.
    - Liability clauses that apportion risk fairly between public and private entities in case of system failures or cyber-attacks.
    - Mandatory clauses for algorithmic transparency, requiring vendors to provide "explainability" features for their AI systems.
4. **Establishing Institutional Mechanisms:**
    - **City-Level Data Protection Officers (DPOs):** Each SPV should be required to appoint an independent DPO with the authority to monitor compliance with data protection laws.
    - **Algorithmic Auditing Panels:** Independent, multi-stakeholder panels comprising technologists, lawyers, and civil society representatives should be constituted to audit the algorithms used in public decision-making for fairness, bias, and accuracy.

CONCLUSION

The Smart Cities Mission holds the potential to redefine urban living in India, promising efficiency, sustainability, and improved quality of life. However, this technological leap cannot be taken at the cost of eroding fundamental rights, democratic accountability, and social equity. The current legal framework is a patchwork of outdated and ill-fitting statutes, creating a landscape of significant risk and uncertainty.

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This paper has demonstrated that the challenges are profound and interconnected. The weak spots in data protection enable surveillance, the gaps in cybersecurity threaten public safety, the ambiguities in IPR risk the privatization of public goods, and the lack of algorithmic accountability undermines the rule of law. The newly minted DPDPA, 2023, is a necessary but insufficient piece of the puzzle.

Building a smart city is not merely an engineering challenge; it is a socio-legal one. The hardware of sensors and fiber optics must be supported by the software of just laws and accountable institutions. India stands at a crossroads. It can either allow its smart cities to become laboratories of unchecked technological power and corporate control, or it can seize this moment to pioneer a new model of digital urban governance that is transparent, participatory, and rooted in constitutional values. The choice will determine whether the cities of the future are smart for all their citizens or merely intelligent cages.

REFERENCES

- Bhattacharya, S., & Rathi, S. (2015). *Reconciling the right to the city and the smart city: A study of the Smart Cities Mission in India*. Centre for Policy Research. https://cprindia.org/briefsreports/reconciling-the-right-to-the-city-and-the-smart-city/
- *Digital Personal Data Protection Act, 2023*, No. 22 of 2023, Acts of Parliament, 2023 (India). https://www.meity.gov.in/data-protection
- Graham, M., & Mann, L. (2018). *The cybersecurity of smart cities: A review of the literature*. The Alan Turing Institute. https://www.turing.ac.uk/research/publications/cyber-security-smart-cities-review-literature
- Green, B. (2019). *The smart enough city: Putting technology in its place to reclaim our urban future*. MIT Press.

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2025
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

- *Information Technology Act, 2000*, No. 21 of 2000, Acts of Parliament, 2000 (India). https://www.meity.gov.in/content/information-technology-act-2000
- *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
- Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal, 79*(1), 1–14. https://doi.org/10.1007/s10708-013-9516-8
- Ministry of Housing and Urban Affairs. (2015). *Smart Cities Mission statement & guidelines*. Government of India. https://smartcities.gov.in/
- Ministry of Housing and Urban Affairs. (2021). *India's urban future: A perspective on urban development*. Government of India. https://mohua.gov.in/
- Sharma, R., & Khanna, S. (2022). The illusion of consent in the smart city. *Indian Journal of Law and Technology, 18*(1), 45-67.
- *State of West Bengal v. Anwar Ali Sarkar*, AIR 1952 SC 75.
- Suresh, A. (2021). *Facial recognition technology in India: A primer*. The Centre for Internet and Society. https://cis-india.org/internet-governance/facial-recognition-technology-in-india-a-primer