The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

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

LEGAL ASPECTS OF THE DIGITAL ECONOMY IN INDIA: DATA GOVERNANCE AND COMMUNITY DATA STEWARDSHIP FOR URBAN DATA

-Dhaarna Rawat

ABSTRACT

India's digital economy is increasingly dependent on data infrastructures embedded in urban life, including integrated command-and-control centres, sensor-based mobility systems, and surveillance networks. India's data governance frameworks, including the Digital Personal Data Protection Act 2023, the Non-Personal Data Governance Framework, and the National Data Governance Framework Policy 2022, address these urban and community datasets only in a fragmented and cautious manner. This article critically examines India's emerging data governance architecture, with a focus on community data and its legal regulation. It argues that while India has made progress in protecting individual data rights, it still lacks coherent legal and policy frameworks for recognizing and governing community data rights.

INTRODUCTION

Urban data infrastructures are playing an increasingly important role in governing India's digital economy and are raising urgent questions about data ownership, reuse, and accountability[1]. The Digital Personal Data Protection Act 2023 creates a rights-based regime around personal data, while the proposed non-personal data and national data governance frameworks focus on non-personal and anonymised data[2]. Both frameworks acknowledge

[1] Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE, https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf

[2] PRS Legislative Research, *Revised Draft Non-Personal Data Governance Framework*, Report Summary (July 27, 2020), https://prsindia.org/policy/report-summaries/revised-draft-non-personal-data-governance-framework; Press Information Bureau, Gov't of India, *National Data Governance Framework Policy* (Press Release, July 26, 2022), https://pib.gov.in/PressReleasePage.aspx?PRID=1845318.

community data but fail to provide any clear legal regime governing it[3]. This gap has led academics and policy organisations to explore data stewardship models, where intermediaries such as data trusts, cooperatives, or other governance platforms[4] mediate the interests of defined communities. At the same time, initiatives to develop city-specific urban data-sharing infrastructure, such as the IUDX platform, highlight the limited scope of public involvement and accountability in managing urban data[5]. Building on these debates, this paper explores how community data is framed under Indian law in urban contexts, how it is emerging around new urban data platforms, and what legal developments would be necessary to govern it as a public common rather than as state or private property.

MAPPING THE LEGAL LANDSCAPE OF DATA GOVERNANCE IN INDIA

India's data governance regime is split across the DPDP Act, the IT Act, and the proposed non-personal data framework. With respect to implementing appropriate technical and organisational measures, ensuring personal data is accurate and complete when used in making decisions about data principals, notifying both the Data Protection Board and data principals when a breach of personal data has occurred, and requiring deletion of personal data upon fulfilling the purpose or upon withdrawing of consent unless a legal obligation to retain it exists, the data fiduciary is made responsible for any non-compliance[6]. The DPDP Act also allows for the appointment of 'significant data fiduciaries' through central government order. These data fiduciaries are further required to carry out data protection impact assessments and appoint data protection officers, and they must also carry out data protection audits. All these duties and responsibilities are directly applicable to municipal authorities, special purpose vehicles for smart cities, private service providers handling urban residents' personal data for large-scale surveillance, public transportation, and digital service delivery.

Outside the DPDP regime, the IT Act and the 2011 rules on reasonable security practices and sensitive personal data remain a baseline set of obligations on companies, including security

---

[3]Software Freedom Law Ctr., India, *Our Comments on Revised Non-Personal Data Governance Framework Report* (2020), https://sflc.in/our-comments-revised-nonpersonal-data-governance-framework-report/

[4]Vidhi Centre for Legal Policy, Data Stewardship for Non-Personal Data in India: A Position Paper on Data Trusts (Nov. 19, 2020),https://vidhilegalpolicy.in/research/data-stewardship-for-non-personal-data-in-india/; Aapti Institute, Fostering Participatory Data Stewardship (June 6, 2023), https://aapti.in/fostering-participatory-data-stewardship/

[5]India Urban Data Exchange, Data Exchange Framework for Indian Smart Cities (discussion paper), https://iudx.org.in/archives/Discussion_Paper-Data_Exchange_Framework_for_Indian_Smart_Cities.pdf.

[6]Digital Personal Data Protection Act, 2023, No. 22 of 2023, Gazette of India, Extra., pt. II, sec. 1 (Aug. 11, 2023), https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf

and liability in the form of compensation for damages caused by wrongful loss as a result of negligence[7]. In tandem, the Ministry of Electronics and Information Technology's Committee of Experts on Non-Personal Data has proposed an independent regulatory framework that seeks to delineate public, private and community non-personal data, envisages a Non-Personal Data Authority with powers to compel data sharing and deal with potential harms arising from the wrongful use of such data, while the NDGFP and its commentary proposes an India Data Management Office, to both systematize government data management and administer an India Datasets program that seeks to provide large repositories of anonymised non-personal data for research and innovation. These instruments, taken together, create a piecemeal system of data governance under different models of rights, duties, and state-community relationships. On the one hand, individual data rights appear increasingly codified, and individual protection increasingly legally enforceable; on the other hand, non-personal and community data rights, and particularly non-personal and community data rights in urban space, are mediated through evolving policy and draft frameworks rather than codified legal rights. The relationship between what might be termed 'hard' rights for individual data, and 'softer' rights for community and non-personal data is key to understanding the challenges of urban data governance and community data stewardship.

CONCEPTUALISING COMMUNITY DATA AND DATA STEWARDSHIP

The Non-Personal Data Governance Framework discusses community non-personal data, data relating to groups of individuals generated from usage of a product or service or activities in a public space[8]. Aapti has presented data stewardship as a model 'places individuals and communities at the center of decisions about data collection, use and sharing-often involving intermediaries such as data trusts, cooperatives, or fiduciaries'[9]. Vidhi has discussed in its position paper how data trusts could be structured in the Indian legal landscape, referencing provisions from Indian Trusts Act, Societies, and Section 8 companies to guarantee that data trustees have the fiduciary duty to act in the best interests of the group beneficiaries[10]. These models indicate a move away from access-based models of open data toward models that

[7] Information Technology Act, 2000, No. 21 of 2000, Gazette of India, Extra., pt. II, sec. 1 (June 9, 2000); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, Extra., pt. II, sec. 3(i) (Apr. 11, 2011)
[8] PRS Legislative Research, Revised Draft Non-Personal Data Governance Framework, supra note 2.
[9] Aapti Institute, Fostering Participatory Data Stewardship, supra note 4.
[10] Vidhi Centre for Legal Policy, Data Stewardship for Non-Personal Data in India, supra note 4.

require fiduciary duties, representation and accountability. However, stewardship remains underdefined in law and difficult to implement.

URBAN DATA INFRASTRUCTURES: SMART CITIES, IUDX AND URBAN DATA PLATFORMS

Urban data infrastructures, especially smart-city systems, create both service benefits and privacy concerns because data are increasingly shared across public and private actors. To provide a framework to these developing systems is one of the key objectives of the India Urban Data Exchange. IUDX is an open-source software platform, designed to provide a secure, authenticated and governed manner of exchanging data between municipal authorities, utility services, transport agencies, private companies and other urban actors via standardized interfaces (APIs) and mechanisms to control data access. A discussion paper on IUDX highlights the platforms respect for the data provider's intent and permissions and the use of various identification, authentication and authorization protocols and policies to control access to data sets. Ideally, this system can facilitate beneficial uses of data on the city including research, innovation and coordination between departments, while decreasing ad-hoc arrangements for data sharing.

National Urban Data Platforms and city level data portals push this logic further by pooling urban data from multiple sources into common environments for planning and analysis. In case studies of implementation in cities like Satna it is possible to see how remote sensing and municipal records can be brought together for analysis of urban growth, change of land use, and service deficiencies, information that then enters the planning process[11]. But critics highlight how the governance around these platforms tends to be technocratic and vendor driven and lack transparency with regard to data flows, algorithmic tools and structures of decision making. The research conducted by Bot Populi on Indian smart cities argues that such projects could result in the increasing of democratic deficit by migrating the functions of certain governance processes into special purpose vehicles and opaque technological systems that are 'removed at an arm's length from the elected bodies in municipalities'[12].

[11] City Transitions & ISCN, Insights from Deployment of National Urban Data Platforms in India (2021), https://city-transitions.global/wp-content/uploads/ISCN-study_DataPlatformsIndia.pdf
[12] Bot Populi, Smart Cities in India: Of Data Governance and Democratic Deficits (Nov. 18, 2021), https://botpopuli.net/smart-cities-in-india-of-data-governance-and-democratic-deficits/.

From the viewpoint of community based data stewardship these urban data infrastructures can be both double and triple-edged. They could, in theory, function as shared repositories governed by community-oriented trustees or by cooperative entities representing residents' interests in matters of data access and reuse. The contracts and legal structures of many smart city and data platforms, however, primarily take into account the interests of public and corporate actors and leave residents' interests to be negotiated, if at all, through bland data privacy or open data policies. Consequently, we live in a world where urban data are crucial for the operations of cities and the economy, and yet residents lack power over urban data.

CRITICAL ISSUES IN LEGAL DESIGN: RIGHTS, POWER AND PARTICIPATION

The core dichotomy within the Indian data governance space is between comparatively strong individual rights in the DPDP Act, and very thin notions of community or group rights on non-personal and urban data. While the DPDP Act grants rights over one's personal data (access, correction, erasure, withdrawal of consent and the right to complain to the Data Protection Board) to data principals, the references in the NPD framework on community data are primarily in terms of communities being recipients of obligatory data sharing, not as rights holders with concrete rights of refusal of harmful uses or to demand specific governance regimes[13]. Academic and civil society critics fear this will risk community data being treated as a public resource for state/corporate innovation rather than as an issue that demands that the politics of representation, power, and justice be navigated. Smart city and urban data projects bring this tension into concrete view. An analysis of smart city contracts and the design of institutional mechanisms for smart cities points to special purpose vehicles and concession agreements as ways of marginalizing accountability at the municipal level by placing authority in small boards and project management teams, usually with a significant degree of corporate influence. In the area of smart cities and democracy, scholarship highlights concerns of vendor driven smart city projects, lack of transparent procedures and tenders, and invisible technological decisions that can undermine public deliberation, entrench surveillance and create difficult to escape dependencies on private platforms[14]. Existing tools of law such as the IT Act, the municipal laws and general constitutional remedies may offer piecemeal protections

[13] See supra notes 1–3.
[14] See Nat’l Endowment for Democracy, Smart Cities and Democratic Vulnerabilities (2022).

to citizens to push back against intrusive data practices and demand a real accounting for their urban data.

However, capacity and implementation constraints also add layers of complexity. The Aapti research into community participation in data stewardship, identifies the constraints faced by data stewards in designing participatory data governance models and ensuring community participation in the long-term beyond pilot projects, particularly when a deficit in resources and technical expertise exists[15]. Most urban local bodies are generally under-resourced, with small legal and technical departments, and are reliant on external consultants. Additionally, it is unlikely that there are systematic internal policies, even post the DPDP Act, for data protection and non-personal data governance. These limitations would naturally restrict the operationalisation of community data stewardship models within urban data infrastructures, thus ensuring dominance of the state and private sector in this space.

TOWARDS COMMUNITY DATA STEWARDSHIP FOR URBAN INDIA: DIRECTIONS FOR REFORM

If urban data is to be managed as a common pool resource balancing individual and common interests, Indian law and policy will have to move beyond generic references to community data to develop more tangible rights and institutional structures. One important step would be to institutionalize community data rights within a new piece of non-personal data legislation or in the detailed implementation framework for the NDGFP[16]. These rights could include the right to be consulted in the terms of any data sharing arrangements, the right to nominate and elect a data trustee, and the right to challenge the use of community data which leads to community-level harms or re-entrenches exclusion. This wouldn't answer every definitional dispute over what a community is, but it would signify that communities are something more than passive beneficiaries of data driven governance.

A second avenue would be to bake principles of stewardship directly into the management of urban data platforms. Building on some proposals from Vidhi and Aapti, legislative bodies and municipalities could pilot legally recognized data trusts or cooperative organizations for certain

[15] Aapti Institute, Paradigms for Community Participation in Data Stewardship (May 29, 2023), https://aapti.in/g0-paradigms-for-community-participation-in-data-stewardship/.
[16] See supra note 2.

types of urban data (like mobility data, environmental data, and slums upgrading data)[17]. These organizations could hold and negotiate for access to data on behalf of specified communities, participate in governance boards such as those of IUDX and National Urban Data Platforms, and manage transparent mechanisms for conflict resolution and complaint handling. Contracts for smart city system procurement and concessions should also impose duties on vendors to adhere to steward-based governance models and adopt privacy by design and data minimisation standards that exceed statutory minimums.

Finally, implementation of the DPDP Act in urban areas would be critical. The introduction of a city-specific data protection framework, specific sectoral regulations on surveillance, mobility and welfare systems and a set of capacity building programs aimed at municipal officials and smart city staff would help convert general fiduciary duties into tangible practices. Active involvement of civil society groups, resident associations and informal sector worker unions in formulating the framework would be vital, not only to ensure that the technical safeguards accommodate lived realities, but to enhance trust in digital urban governance processes. As Indian cities become increasingly data intensive, present day decisions on data governance and community stewardship will guide not only the growth of the digital economy, but also the urban daily reality of citizenship.

[17] See super note 4.