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

Data Governance and Organizational responsibility under India's new digital laws

~ Mayank Chaurasia

Introduction

Data has always been a central infrastructure of governance, commerce, and social organizations in the contemporary India. Public welfare delivery, financial systems, healthcare administration, employment platforms, and digital marketplaces, all increasingly rely on the collection and processing on large volumes of personal database. As a result of this, data is no longer just a neutral informational asset; Instead, it has emerged as a source of economic power, institutional control, and regulatory concern, where the governance of data is therefore raises questions not only of privacy, but also over organizational responsibility, accountability, and democratic legitimacy[1].

India's recent digital legislative developments most notably the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act) represents a significant attempt towards the regulation evolution landscape through law[2]. This act introduces a formal framework that governs the collection, processing, and protection of personal data by both the public and private entities; however, the effectiveness of this framework is dependent less on statutory text and more on how the organizations internalize these legal obligations within their governance and management structures.

This article examines the data governance in India through a combined framework of law and management, where it argues that India's new digital laws impose more substantive responsibilities on organizations that go beyond the procedural compliance. The data governance must be understood as a governance function that is concerned with power, risk, and institutional accountability rather than just as a narrow legal or technical exercise.

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019).

[2] Digital Personal Data Protection Act, 2023, No. 22 of 2023, INDIA CODE.

Data Governance as a Legal and Organizational Concept

Data governance refers to the rules, processes, and institutional arrangements determining that how the data is collected, used, stores, shared, and protected. Traditionally, the organizations have treated data governance as a technical function that is managed by information technology departments or other legal compliance teams. This approach is increasingly adequate in a digital economy where the data practices directly affects the individual autonomy, market competition, and public trust[3].

From a legal point of view, data governance is concerned with rights and obligations, where, it addresses who controls data, on what grounds data may be processed, and what are the remedies available in cases of misuse. From a management point of view, data governance involves a strategic decision making, internal controls, risk management, and organizational culture. When all these perspectives are integrated, data governance emerge as a core governance responsibility rather than a peripheral compliance task.

India's digital laws are implicitly recognizing this shift by introducing the concept of "*Digital Fiduciaries"* , the DPDP Act reframes the organizations as an entities entrusted with personal data rather than owners of it[4]. This fiduciary framing emphasize care, responsibility, and accountability, aligning the data governance with a broader principles of corporate and institutional governance.

Constitutional Foundations of Data Protection in India

India's data governance framework is firmly rooted in a constitutional jurisprudence. In a case of "*Justice K.S. Puttaswamy (Retd.) v. Union of India",* the supreme court recognizes the right to privacy as an intrinsic part of the right to life and personal liberty under the Article 21 of the Constitution[5], and emphasized that informational privacy is essential to the dignity, autonomy, and democratic participation in a digital society.

The court also clarifies here that the right to privacy is not absolute in nature, instead, any restriction of privacy must first satisfy the tests legality, necessity and proportionality[6]. This framework requires both of the state and private actors to justify the data collection and processing through the legitimate aims and minimal intrusion. This proportionality doctrine was earlier developed in cases such as *"Maneka Gandhi v. Union of India"* has become central to digital governance in India[7].

More importantly, the *Puttaswamy* Judgement highlighted concerns about the asymmetries of informational power. Here, the court eventually warned that any unchecked data accumulation by the state or corporations could enable surveillance and control incompatible with democratic

[3] OECD, *Privacy Guidelines* (2013).
[4] Digital Personal Data Protection Act, 2023 §§ 2–4.
[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[6] Id.
[7] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248.

freedoms[8]. These concerns are directly informing the legal responsibilities imposed on organizations under the India's digital laws.

The Digital Personal Data Protection Act, 2023

The DPDP Act, 2023 is India's one of the first comprehensive statute regulating personal data protection act, that established a consent-based framework for data processing and recognizes lawful grounds for processing personal data and grants rights to individuals termed as "*data principles"* including the right to access information, correction of inaccurate data, erasure, and grievance redressal[9].

A defining feature of the Act is the classification of these entities as "*data fiduciaries"* and "*significant Data Fiduciaries."* These data fiduciaries are required to process data lawfully, ensure accuracy, implement reasonable security safeguards, and respond to requests from data principals[10]. Significant data fiduciaries that are identified on the basis of volume and sensitivity of data processed are subject to additional obligations such as appointing Data Protection Officers, who conducts data protection impact assessments and undergoing periodic audits[11].

These requirements represents an attempt to embed accountability mechanisms within the organizational structures. By mandating the internal roles and assessments, this act seeks to integrate legal compliance into a managerial decision-making rather than treating it as an external obligation, however, the act also grants broad exemptions to the state for purposed such as national security and public order[12]. From a governance point of view, this creates an uneven accountability framework that raises the concerns about selective application of data protection principles.

Organizational Responsibility and Internal Governance Structures

Legal Compliance alone is insufficient to ensure a responsible data governance. Organizations here must translate statutory duties into internal governance practices that could shape the everyday decision-making. This requires a firm shift from a reactive compliance towards a proactive responsibility.

Firstly, the data governance must be anchored at the highest levels of organizational leadership, where the decisions regarding data collection, retention, and monetization are strategic choices with a legal, ethical, and reputational consequences. Treating the data governance as a technical issue delegated to lower level departments eventually undermines accountability. And Corporate

[8] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[9] Digital Personal Data Protection Act, 2023 ch. II.
[10] Id. §§ 8–10.
[11] Id. § 10.
[12] Id. § 17.

governance frameworks increasingly recognizes the data as a core enterprise risk alongside with the financial and operational risks[13].

Secondly, the internal accountability mechanism are also essential. The appointment of data protection officers under the DPDP Act reflects the recognition of this need. However the effectiveness of such roles depends on institutional independence and authority. If DPOs lacks the access to decision making processes or face any pressure to prioritize commercial interests, governance objectives will be eventually compromised and unfulfilled.

Thirdly, the organizational culture also plays a critical role in data governance. Employees across the departments interact with data systems, but still awareness of data protection principles is often limited. Embedding the concepts such as data minimization, purpose limitation and privacy by design requires sustained training and ethical engagement across the organization[14].

Data Governance, Market Power, and Inequality

Data governance is seen to be closely linked to questions of market power and inequality. Data-intensive business models allows the organizations to derive the competitive advantages through scale, analytics, and network effects. In such contexts, data functions as a barrier to entry that reinforces the market concentration and limiting competition[15].

Consent based data protection models, while they are legally significant, are often seen to be a failure in order to address these structural imbalances, here, the individuals rarely possesses the bargaining power or informational capacity to meaningfully negotiate the use of data, particularly when access to the essential services is conditioned on consent. Therefore, organizational responsibility extends beyond the formal consent towards the substantive fairness in data practices.

From a law and management perspective, this raises some important questions about corporate responsibility in digital markets. Competition law and data protection law increasingly intersect in addressing algorithmic decision making, platform dominance, and discriminatory outcomes[16]. Organizations must assess the broader social impact of data driven practices, especially where they are affecting the access to employment, credit, or other public services.

State Data Practices and Public Sector Accountability

While private organizations dominate the discussions on data governance, other state data practices raises equally significant concerns. Government databases related to the welfare delivery, identity verification, and surveillance involves large scale processing of sensitive personal data, and

[13] OECD, *Data-Driven Innovation and Corporate Governance* (2015).
[14] Julie E. Cohen, *Between Truth and Power* (2019)
[15] Competition Act, No. 12 of 2003, INDIA CODE.
[16] Danielle Keats Citron & Frank Pasquale, *The Scored Society*, 89 Wash. L. Rev. 1 (2014).

systems such as Aadhar illustrates both the efficiency gains and the governance risks that are associated with centralized data infrastructure[17].

Although the DPDP act is applied to the state, its broader exemptions dilute the enforceability, which eventually creates a two-tier system of accountability in which private actors faces stringent compliance obligations, while state agencies enjoy discretionary leeway. This asymmetry undermines the principle that the data protection is fundamentally about limiting powers, regardless of who exercises it[18].

Therefore, the organizational responsibility in the public sector must be understood as a constitutional obligation, where the state agencies are custodians of citizens' data and they must adhere to standards of transparency, proportionality, and fairness. Judicial review and independent oversight remains an essential mechanism for ensuring the accountability in public sector data governance.

Integrating Law and Management: Responsible Data Stewardship

Effective data governance requires an integration between certain legal norms and managerial practices. The law establishes rights, duties, and enforcement mechanisms, whereas on the other hand, managerial operationalizes these norms through organizational design, incentives, and controls.

Responsible data stewardship involves the recognition of data as a social resource rather than a purely proprietary asset, where organizations must balance the innovation and efficiency with respect for individual autonomy and collective welfare, and this balance cannot be achieved through compliance alone as it requires ethical judgement, institutional accountability, and long-term governance planning[19].

International experience also suggests that the organizations adopting proactive data governance frameworks are benefit from greater trust, reduced regulatory risk, and institutional legitimacy. In contract, the reactive compliance approaches are often lead to legal exposure and reputational harm, however, India's digital laws provide an opportunity for organizations to rethink data governance as a central element of responsible management.

Conclusion

India's new digital laws represents a significant step towards regulating data practices in an increasingly digital society. By imposing fiduciary like obligations on organizations and recognizing individual data rights, the DPDP Act seen as reshaping the legal landscape of data

[17] *Justice K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 SCC 1
[18] UN General Assembly, *The Right to Privacy in the Digital Age*, G.A. Res. 68/167 (2013).
[19] Karl Polanyi, *The Great Transformation* (1944)

governance, however, the success of this framework depends on how organizations internalize responsibility beyond just a formal compliance.

Ultimately, data governance is a question of power, accountability, and institutional design. Organizations that collects and processes data exercises a significant influence over individuals and markets, which aligns these practices with constitutional values, legal norms, and ethical governance, which is essential for sustaining trust and democratic legitimacy. As data becomes central to governance and economic organization, it thus eventually ensures responsible organizational stewardship, which is no longer optional in this sense; it is a legal and institutional necessity.