DATA PRIVACY AND CORPORATE COMPLIANCE IN INDIA: CONSTITUTIONAL AND GOVERNANCE PERSPECTIVES ON THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Harshita Aggarwal, Bharati Vidyapeeth Institute of Management and Research (BVIMR)

Parth Aggarwal, Bharati Vidyapeeth Institute of Management and Research (BVIMR)

ABSTRACT

The Digital Personal Data Protection Act, 2023 ("DPDP Act") is India's first dedicated statute on digital personal data and is the legislative culmination of a constitutional debate that began in earnest with the Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India.[1] The Act's stated objective is to regulate the processing of digital personal data in a manner that balances individuals' right to protect their data with the need to use such data for lawful purposes.[2] This balance is not a neutral technical exercise. It redistributes power between data principals, corporations and the State, and it reshapes the internal governance of Indian companies that rely on data-intensive business models.[3]

This article offers a critical study of the DPDP Act from the perspective of Indian corporate compliance, located within the broader constitutional and comparative context.[4] It argues that the Act is best understood as a governance statute: it creates duties concerning consent, legitimate uses, accuracy, security, breach notification, erasure, children's data and Significant Data Fiduciaries, and it establishes the Data Protection Board of India as an adjudicatory body with power to impose substantial penalties.[5] At the same time, the statute suffers from structural weaknesses, including heavy reliance on delegated legislation, broad executive exemptions, an

[1]Digital Personal Data Protection Act, 2023, No. 22 of 2023, Gazette of India, Aug. 11, 2023 (India); *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

[2] Digital Personal Data Protection Act, 2023, pmbl.; id. § 4.

[3] See Digital Personal Data Protection Act, 2023, §§ 2(6), 2(13), 4, 7, 8, 10 (reflecting allocation of obligations among data principals, data fiduciaries and the State).

[4] See generally *Puttaswamy (Retd.)*, (2017) 10 SCC 1; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[5] Digital Personal Data Protection Act, 2023, §§ 4–10, 18, Sch. (setting out duties of data fiduciaries, Significant Data Fiduciaries and the powers of the Data Protection Board of India).

under-specified institutional design for the Board and limited articulation of individual rights compared to leading global regimes.[6]

Drawing on Puttaswamy, later proportionality jurisprudence, comparative data protection frameworks such as the EU General Data Protection Regulation and Asian personal data laws, and emerging corporate risk practice, the article contends that the DPDP Act's success will be determined less by its existence and more by its implementation.[7] If rulemaking, adjudication and corporate adaptation are guided by constitutional proportionality, institutional independence, sectoral coordination and genuine "privacy by design", the Act can become a meaningful foundation for digital constitutionalism in India.[8] If not, it risks becoming a formal licence for continued data extraction under the vocabulary of consent and compliance.[9]

I. Introduction

Data has moved from being a by-product of economic activity to being its underlying infrastructure.[10] Indian businesses collect, generate, analyse, monetise and share personal data through e-commerce platforms, digital lending and payments, insurtech products, health-technology applications, employment systems, logistics networks, ride-hailing services, education technology and cloud-based enterprise tools.[11] Data flows underpin targeted advertising, credit scoring, fraud detection, recommendation engines, automated hiring and AI-driven analytics.[12] In such an environment, the question is not whether data should be regulated, but how law ought to allocate responsibility over data among individuals, corporations and the State.[13]

Until recently, Indian data protection rules were housed in scattered provisions such as section 43A and the Information Technology (Reasonable Security Practices and Procedures and

[6] Id. §§ 17–18 (exemptions and Board design); cf. GDPR arts. 12–22 (rights) (illustrating broader individual rights catalog).
[7] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1; *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1 (India); *Modern Dental Coll. & Research Ctr. v. State of M.P.*, (2016) 7 SCC 353 (India).
[8] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 271–72 (Chandrachud, J.) (discussing proportionality and constitutional limits on State power); *Modern Dental Coll.*, (2016) 7 SCC 353, 384–85 (setting out structured proportionality test).
[9] Cf. Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 8–12 (PublicAffairs 2019).
[10] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 194–96 (Chandrachud, J.) (noting that in the digital age, data has become central to economic and social life).
[11] See id. at 193–97; NITI Aayog, *India's Trillion-Dollar Digital Opportunity* 3–6 (2019) (describing data-driven sectors of the Indian economy).
[12] NITI Aayog, *India's Trillion-Dollar Digital Opportunity*, supra note 11, at 7–11.
[13] Cf. *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 193–97 (linking data-centric technologies to privacy concerns).

Sensitive Personal Data or Information) Rules, 2011, supplemented by sectoral norms for finance, telecom, health and e-commerce.[14] That patchwork was increasingly regarded as insufficient after the Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, where a nine-judge bench affirmed privacy as a fundamental right intrinsic to life and personal liberty under Article 21 and closely connected to dignity and autonomy.[15] Once privacy acquired explicit constitutional status, the need for a dedicated and comprehensive data protection statute became unavoidable.[16]

The DPDP Act is Parliament's principal response to this constitutional moment.[17] It is a relatively concise statute that applies to digital personal data processed in India, and to certain extra-territorial processing connected with the offering of goods or services to individuals in India.[18] It adopts a compact set of concepts—data principal, data fiduciary, data processor, consent, legitimate use, Significant Data Fiduciary—and establishes a new adjudicatory body, the Data Protection Board of India.[19] The Act's drafting strategy is to prescribe high-level duties and powers while leaving detailed operational questions to rules and executive notifications.[20]

This article advances three core claims. First, the DPDP Act should be read primarily as a governance and compliance statute rather than as a mere rights-declaratory instrument.[21] Its real impact will be felt in boardrooms, compliance functions, product design teams and vendor contracts.[22] Secondly, the statute's design reflects a deliberate trade-off between breadth of coverage and institutional ambition. It is more limited in scope and in its rights catalogue than some global models, but it centralises enforcement and penalties in a significant way.[23] Thirdly, the law's normative promise is undermined by its exemption architecture, its reliance on

[14] Information Technology Act, 2000, No. 21 of 2000, § 43A (India); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gazette of India, June 13, 2011, pt. II, sec. 3(i).
[15] *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 262–63 (Chandrachud, J.) (holding that privacy is intrinsic to life and personal liberty under art. 21 and closely linked to dignity).
[16] See id. at 266–67 (urging the Union of India to examine and put into place a robust data protection regime).
[17] See Digital Personal Data Protection Act, 2023, pmbl.; Statement of Objects and Reasons, Digital Personal Data Protection Bill, 2023, Bill No. 131 of 2023 (Lok Sabha).
[18] Digital Personal Data Protection Act, 2023, § 3(1)–(2).
[19] Id. §§ 2(6), 2(9), 2(13), 4–7, 10, 18.
[20] Id. §§ 4–10, 22–25, 40 (empowering the Central Government to make rules on key operational questions).
[21] See Graham Greenleaf, *Global Data Privacy Laws 2024: Despite Problems, 162 Laws Show GDPR Dominance*, 190 Privacy Laws & Bus. Int'l Rep. 1, 12–14 (2024) (discussing governance-oriented data protection frameworks, including India's DPDP Act).
[22] Id.; see also EY, *Decoding the Digital Personal Data Protection Act, 2023* 6–8 (2025) (highlighting impact on corporate governance and compliance functions).
[23]Digital Personal Data Protection Act, 2023, §§ 3–4, 11–15, Sch.; cf. GDPR arts. 5–6, 12–23, 83–84.

delegated legislation and the uncertain independence of the Board.[24] Without careful implementation and doctrinal development, the risk is that the Act may legitimise extensive data processing while delivering only partial realisation of constitutional privacy.[25]

The structure of the paper is as follows. Part II explains the constitutional foundation of data privacy in India, focusing on *Puttaswamy* and proportionality-based rights review.[26] Part III traces the legislative evolution of the DPDP Act and outlines its core structure.[27] Part IV examines the Act's substantive provisions on consent, legitimate uses and individual rights.[28] Part V turns to corporate compliance obligations, especially for data fiduciaries and Significant Data Fiduciaries.[29] Part VI analyses the enforcement framework and institutional design of the Data Protection Board.[30] Part VII offers comparative reflections on the GDPR, Singapore's PDPA and related regimes.[31] Part VIII focuses on exemptions, State power and proportionality.[32] Part IX sets out a set of reform proposals, and Part X concludes.[33]

II. Constitutional Foundation of Data Privacy in India

A. From scattered privacy references to *Puttaswamy*

Long before the DPDP Act was conceived, Indian constitutional jurisprudence had grappled with aspects of privacy, albeit in fragmented ways.[34] In *Kharak Singh v. State of U.P.*, the Supreme Court dealt with police surveillance practices but delivered a split opinion on whether the Constitution recognised a right to privacy.[35] Later decisions such as *Gobind v. State of M.P.* cautiously accepted that aspects of privacy can be read into the guaranteed freedoms, subject to restrictions.[36] In *R. Rajagopal v. State of T.N.*, the Court acknowledged that citizens have a right "to be let alone" with respect to publication of life stories without consent, indicating an

[24] Digital Personal Data Protection Act, 2023, §§ 17–18.
[25] Cf. *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 193–97 (warning against formal compliance that fails to secure substantive privacy).
[26] See infra Part II.
[27] See infra Part III.
[28] See infra Part IV.
[29] See infra Part V.
[30] See infra Part VI.
[31] See infra Part VII.
[32] See infra Part VIII.
[33] See infra Part IX–X.
[34] See generally Gautam Bhatia, *Privacy and the Indian Constitution*, in *The Transformative Constitution* 285–312 (Navroz K. Seervai et al. eds., 2019).
[35] *Kharak Singh v. State of U.P.*, AIR 1963 SC 1295 (India).
[36] *Gobind v. State of M.P.*, (1975) 2 SCC 148 (India).

informational dimension to privacy.[37]

Similarly, in *People's Union for Civil Liberties (PUCL) v. Union of India*, the Court examined telephone tapping and held that, although the State could intercept communications for legitimate purposes, any such interference must be accompanied by procedural safeguards to minimise abuse.[38] These early cases together recognised elements of spatial, decisional and informational privacy, but the Court stopped short of explicitly declaring privacy to be an independent fundamental right.[39]

B. The *Puttaswamy* moment

This position changed decisively in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[40] A nine-judge bench unanimously held that privacy is a constitutionally protected right that emanates from the guarantees of life, personal liberty, equality and dignity in Part III of the Constitution.[41] The judgment rejected the earlier view in *M.P. Sharma* and the majority in *Kharak Singh* that privacy lacked textual basis.[42] It treated privacy as a basic condition for the exercise of other freedoms and recognised informational self-determination as a central element in a data-driven society.[43]

The Court in *Puttaswamy* articulated several key propositions. First, it affirmed that informational privacy, including control over personal data, is an aspect of the right to privacy.[44] Secondly, it accepted that both State and non-State actors can infringe privacy, acknowledging the role of private corporations that collect and process data.[45] Thirdly, it endorsed proportionality as the test for evaluating restrictions on privacy: any interference must satisfy legality (existence of law), pursue a legitimate aim, be necessary and proportionate, and

[37] *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632, 648–49 (India) (recognising a right "to be let alone" and informational privacy interests).
[38] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301, 326–27 (India) (laying down procedural safeguards against telephone tapping).
[39] See *Kharak Singh*, AIR 1963 SC 1295 (rejecting an express right to privacy); *Gobind*, (1975) 2 SCC 148; *R. Rajagopal*, (1994) 6 SCC 632; *PUCL*, (1997) 1 SCC 301 (recognising aspects of privacy without declaring a standalone fundamental right).
[40] *Puttaswamy (Retd.)*, (2017) 10 SCC 1.
[41] Id. at 262–63 (Chandrachud, J.) (holding that privacy is protected under arts. 14, 19 & 21).
[42] Id. at 237–40 (overruling *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300, and the majority in *Kharak Singh* to the extent they denied a constitutional right to privacy).
[43] Id. at 248–50, 261–62 (discussing informational self-determination and data-driven technologies).
[44] Id. at 262–64.
[45] Id. at 267–68 (acknowledging threats to privacy from non-State actors and large corporations).

incorporate procedural safeguards.[46]

These propositions are decisive when assessing statutory data protection frameworks.[47] A law that leaves broad discretionary room to the executive to exempt itself from obligations, or that fails to build effective oversight and remedies, may fall short of *Puttaswamy*'s standard even if it appears comprehensive on paper.[48] At the same time, *Puttaswamy* did not purport to draft a full data protection code; it called upon the legislature to frame one.[49]

C. Proportionality in subsequent jurisprudence

After *Puttaswamy*, the Supreme Court has further elaborated proportionality in cases such as *Modern Dental College & Research Centre v. State of M.P.* and the Aadhaar judgment in *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*.[50] In *Modern Dental College*, the Court adopted a structured test requiring that rights-restricting measures pursue a legitimate aim, be suitable to achieve that aim, be the least restrictive among alternative measures and maintain a balance between the importance of achieving the aim and the severity of the rights restriction.[51] The Aadhaar decision applied this framework to a nationwide identity system involving large-scale data collection.[52]

The DPDP Act will inevitably be measured against this proportionality template.[53] Its provisions granting broad exemptions to State instrumentalities and its reliance on delegated legislation will be scrutinised to determine whether they are accompanied by sufficient safeguards, oversight and necessity-based reasoning.[54] While the Act undoubtedly gives privacy a statutory foothold, its constitutional adequacy depends on how its architecture fares under this proportionality analysis.[55]

---

[46] See id. at 270–72; *Modern Dental Coll.*, (2016) 7 SCC 353, 383–85 (adopting a four-part proportionality test).
[47] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 270–73.
[48] Cf. id. at 271–72 (requiring legality, legitimate aim, necessity and proportionality, and procedural safeguards).
[49] See id. at 266–67 (referring to the need for a comprehensive data protection regime).
[50] *Modern Dental Coll.*, (2016) 7 SCC 353; *K.S. Puttaswamy (Aadhaar-5J.) v. Union of India*, (2019) 1 SCC 1.
[51] *Modern Dental Coll.*, (2016) 7 SCC 353, 383–85.
[52] *Puttaswamy (Aadhaar-5J.)*, (2019) 1 SCC 1, 128–30, 196–98 (applying proportionality analysis to the Aadhaar programme).
[53] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 270–72; *Modern Dental Coll.*, (2016) 7 SCC 353.
[54] See Digital Personal Data Protection Act, 2023, §§ 17–18.
[55] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 270–73.

III. Legislative Evolution and Structure of the DPDP Act

A. From policy drafts to enacted statute

India's path toward a data protection law has been protracted.[56] Following *Puttaswamy*, an expert committee chaired by Justice B.N. Srikrishna released a report and a draft Personal Data Protection Bill, 2018, proposing a comprehensive framework covering personal and certain non-personal data, with a Data Protection Authority and detailed rights for data principals.[57] Subsequent versions of the bill were introduced in Parliament, but disagreements over data localisation, State exemptions, regulatory design and economic impact led to withdrawal and re-drafting.[58]

The DPDP Act, enacted in 2023, reflects a change in legislative strategy.[59] Rather than adopting a very detailed and long code, Parliament opted for a shorter statute focused on "digital personal data", leaving non-personal data and several institutional questions for separate treatment.[60] The law aims to provide a relatively simple and implementable framework while allowing the executive to specify details through rules and notifications.[61]

B. Scope and application

The Act applies to the processing of digital personal data within India, where such data is either collected in digital form or collected offline and subsequently digitised.[62] It also applies to processing outside India if that processing is in connection with offering goods or services to individuals within India.[63] This extra-territorial reach is significant for foreign platforms and service providers targeting Indian customers.[64]

---

[56] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 266–67 (calling for a data protection regime); PRS Legislative Research, Report Summary, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 1 (2018) (summarising the Committee's recommendations).
[57] Committee of Experts on Data Protection Framework for India, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 1–4, 29–31 (2018) (Justice B.N. Srikrishna, chair); id. annex (draft Personal Data Protection Bill, 2018).
[58] The Personal Data Protection Bill, 2019, Bill No. 373 of 2019 (India); Press Information Bureau, Cabinet Withdraws Personal Data Protection Bill, 2019 (Aug. 3, 2022).
[59] Digital Personal Data Protection Act, 2023, No. 22 of 2023, Gazette of India, Aug. 11, 2023 (India).
[60] See Ministry of Electronics & Information Technology, *The Digital Personal Data Protection Bill, 2023* (Bill Summary) (2023).
[61] Digital Personal Data Protection Act, 2023, §§ 4–10, 22–25, 40 (rule-making and notification powers).
[62] Id. § 3(1).
[63] Id. § 3(2).
[64] See PRS Legislative Research, *The Digital Personal Data Protection Bill, 2023* – Bill Summary 1–2 (2023) (noting implications for foreign entities offering services in India).

At the same time, the Act carves out certain exclusions. It does not apply to personal data processed for personal or domestic purposes, nor to personal data that has been made publicly available by the data principal or by another person under a legal obligation.[65] These exclusions align with the idea that data protection law should focus on institutional processing rather than purely private acts, but they leave open questions about the boundaries of "domestic" processing in an era of public-facing social media use.[66]

C. Conceptual vocabulary

The statute's conceptual vocabulary is notably lean. A "Data Principal" is the individual to whom the personal data relates; a "Data Fiduciary" is the entity that determines the purpose and means of processing; and a "Data Processor" processes personal data on behalf of a fiduciary.[67] This language emphasises a fiduciary model rather than a purely contractual or ownership model: the entity that decides how and why data is processed is treated as bearing primary responsibility, even if day-to-day operations are outsourced.[68]

Personal data is defined as any data about an identifiable individual, and processing is defined broadly to include collection, storage, use, disclosure, sharing, erasure and destruction by fully or partly automated means.[69] This breadth is appropriate because digital harms often arise from aggregation and reuse rather than from collection alone.[70]

D. Legislative technique: framework with delegation

A striking feature of the DPDP Act is its concise drafting style.[71] Many substantive questions—such as the precise content of reasonable security safeguards, timelines for breach notification, details of age verification and criteria for designation as a Significant Data Fiduciary—are left to rules and executive decisions.[72] This framework-plus-delegation model has advantages: it allows flexibility in a fast-changing technological environment and avoids over-specification

[65] Digital Personal Data Protection Act, 2023, § 3(3).
[66] See Digital Personal Data Protection Act, 2023, § 3(3).
[67] Digital Personal Data Protection Act, 2023, § 2(6), (9), (13).
[68] See id.; cf. Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. Davis L. Rev. 1183, 1205–08 (2016) (developing the fiduciary model for information intermediaries).
[69] Digital Personal Data Protection Act, 2023, § 2(13), (20).
[70] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 248–50 (Chandrachud, J.) (discussing aggregation of personal data and emergent harms).
[71] See Digital Personal Data Protection Act, 2023, passim (Act of 44 sections and a Schedule).
[72] Id. §§ 8(5), 9, 10(2), 22–25, 40 (delegation regarding security safeguards, age verification, Significant Data Fiduciaries and other operational details)

that could quickly become obsolete.[73]

However, there are also constitutional and rule-of-law concerns.[74] Excessive reliance on delegated legislation in an area where fundamental rights are at stake may shift too much normative authority from Parliament to the executive.[75] If major questions about exemptions, enforcement standards or adjudicatory design are left to rules, there is a risk of insufficient democratic deliberation and weaker judicial control over the core architecture of data protection.[76] The challenge is to ensure that delegation respects the limits on abdication of essential legislative functions.[77]

IV. Consent, Legitimate Uses and Individual Rights

A. Consent and its limits

Consent is the primary ground of processing under the DPDP Act.[78] Section 4 requires that personal data be processed only in accordance with the Act and for a lawful purpose on the basis of consent or for certain legitimate uses.[79] Section 6 further provides that consent must be free, specific, informed, unconditional and unambiguous, expressed through a clear affirmative action.[80] Consent requests must be accompanied or preceded by a notice specifying the personal data sought, the purpose of processing, the manner in which the data principal may exercise rights and the mechanism for lodging complaints with the Board.[81]

In theory, this approach rejects passive, bundled or forced consent practices.[82] It aims to ensure that consent is meaningful rather than merely formal.[83] For corporate compliance, this translates into the need for clear and accessible user interfaces, layered notices, granular

[73] See Nandan Kamath & Aman Nahar, Rulemaking for Data Protection: Implementing India's Digital Personal Data Protection Act, 2023, Indian J.L. & Tech. (NLSIU Blog, Apr. 11, 2025) (arguing that delegation can enable technological flexibility).
[74] See generally *In re Delhi Laws Act*, AIR 1951 SC 332 (India) (laying down limits on legislative delegation).
[75] See Tarunabh Khaitan, Throwing the Delegation Doctrine to the Winds, Verfassungsblog (Dec. 5, 2022) (critiquing broad delegation in the draft DPDP Bill, 2022).
[76] See Kamath & Nahar, supra note 73 (warning about executive-dominated rulemaking in core rights areas).
[77] See *In re Delhi Laws Act*, AIR 1951 SC 332; *Avinder Singh v. State of Punjab*, (1979) 1 SCC 137, 144–45 (India) (reaffirming that essential legislative functions cannot be delegated).
[78] Digital Personal Data Protection Act, 2023, § 4.
[79] Id.
[80] Digital Personal Data Protection Act, 2023, § 6(1).
[81] Digital Personal Data Protection Act, 2023, § 5.
[82] See id. §§ 4–6.
[83] See European Data Protection Board, Guidelines 05/2020 on Consent Under Regulation 2016/679, at 9–12 (2020) (insisting on informed, specific and unambiguous consent) (used here comparatively).

consents where appropriate, and robust records of consent and withdrawal.[84]

However, consent-based models face well-known limitations in digital environments.[85] Users frequently face fatigue due to the volume and complexity of consent interactions.[86] Power imbalances, especially in employment and essential service contexts, further weaken the voluntariness of consent.[87] Interface design can manipulate users into granting permissions through dark patterns such as pre-selected options, confusing toggles or misleading visual hierarchies.[88] A purely formal focus on consent risks legitimising data practices that users do not genuinely understand or freely accept.[89]

B. "Certain legitimate uses": statutory grounds beyond consent

Recognising these limitations, the Act does not rely on consent alone.[90] Section 7 enumerates a set of "certain legitimate uses" where processing is permitted without consent, including situations where data is voluntarily provided for a specified purpose and the principal has not indicated refusal; where processing is necessary for State functions; where it is required by law or by court order; and where it is necessary to respond to medical emergencies, public health situations, disasters or employment-related purposes.[91]

Some of these grounds are relatively uncontroversial.[92] Processing required by law or by court order is a standard feature of data protection statutes.[93] Emergency-based processing for medical care or disaster response aligns with the need to protect life and safety.[94] Other grounds, however, are more open-textured.[95] The voluntary-provision clause may be interpreted expansively in everyday service contexts, and the employment-related ground, if

[84] See EY, *Decoding the Digital Personal Data Protection Act, 2023* 10–13 (2025) (advising Indian companies on consent flows and record-keeping).
[85] See Solon Barocas & Helen Nissenbaum, Big Data's End Run Around Anonymity and Consent, in *Privacy, Big Data, and the Public Good* 44, 47–50 (Julia Lane et al. eds., Cambridge Univ. Press 2014).
[86] See Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 563–66 (2008) (documenting consent fatigue).
[87] See GDPR recital 43 (noting that consent may not be freely given where there is a clear imbalance between the data subject and controller).
[88] See OECD, *Dark Commercial Patterns* 11–14 (2022) (cataloguing design practices that manipulate user choice).
[89] See Barocas & Nissenbaum, supra note 85, at 50–52.
[90] Digital Personal Data Protection Act, 2023, § 7.
[91] Id. § 7(a)–(f).
[92] Cf. GDPR art. 6(1)(c)–(d) (legal obligation and vital interests) (for comparative purposes).
[93] See id.; Digital Personal Data Protection Act, 2023, § 7(b)–(c).
[94] Digital Personal Data Protection Act, 2023, § 7(d)–(e).
[95] See id. § 7(a), (f).

construed broadly, could permit extensive workplace monitoring and analytics without meaningful consent.[96]

The design challenge is that legitimate-use provisions are both necessary and potentially dangerous.[97] Without them, everyday governance and commerce would be impossible.[98] With them, there is a risk of eroding the protection that consent is meant to provide.[99] The Act itself provides little further guidance on how these clauses should be interpreted; the burden will fall on regulators, the Board and, ultimately, courts to ensure that "legitimate use" does not become a catch-all justification for intrusive processing.[100]

C. Rights of the data principal

The DPDP Act confers several rights on data principals.[101] Section 11 gives a right to obtain from the data fiduciary a summary of personal data being processed and a list of other data fiduciaries and processors with whom data has been shared.[102] Sections 12 to 14 grant rights to correction, completion, updating and erasure of personal data, subject to certain conditions, and a right to grievance redress before the fiduciary and the Board.[103] Section 13 allows a data principal to nominate another individual to exercise his or her rights in case of death or incapacity.[104]

These rights are important, but they are more modest than the catalogue found in some other regimes.[105] The Act does not explicitly provide for data portability, a general right to object to processing on grounds other than consent withdrawal, or a specific right against automated decision-making.[106] That does not render the law ineffective, but it underscores its focus on baseline protections rather than on a maximalist rights menu.[107] The emphasis is placed on

[96] See Kamath & Nahar, supra note 73 (noting risks of broad legitimate-use clauses).
[97] See GDPR art. 6(1); Digital Personal Data Protection Act, 2023, § 7 (balancing necessity of non-consensual processing with risk).
[98] See id.
[99] See Tarunabh Khaitan, supra note 75 (critiquing enabling structure for executive and private processing).
[100] See Digital Personal Data Protection Act, 2023, §§ 18, 33 (role of Board); see also infra Part VI.
[101] Id. §§ 11–14.
[102] Id. § 11.
[103] Id. §§ 12–14.
[104] Id. § 13.
[105] Cf. GDPR arts. 15–22 (access, rectification, erasure, restriction, portability, objection and automated decision-making).
[106] See Digital Personal Data Protection Act, 2023, §§ 11–14 (omitting explicit data portability and automated decision-making provisions).
[107] See PRS Legislative Research, *The Digital Personal Data Protection Bill, 2023* – Bill Summary 2–3 (contrasting rights under the DPDP Bill with those under the PDP Bill, 2019, and GDPR).

fiduciary duties and complaint resolution rather than on individual proactive control across all contexts.[108]

The Act also adopts an unusual approach by imposing duties on data principals.[109] Section 15 requires data principals to comply with applicable laws, to ensure that they do not impersonate other individuals or suppress material information while providing personal data for establishing identity and to refrain from making false or frivolous grievances or complaints.[110] The inclusion of such duties in a privacy statute is doctrinally interesting.[111] While discouraging abuse of rights is a legitimate concern, there is a risk that the threat of sanctions may deter individuals from invoking their rights or complaining about violations, particularly where there is a power imbalance between data principals and large organisations.[112]

V. Corporate Compliance Under the DPDP Act

A. Duties of data fiduciaries

From the standpoint of corporate governance, Section 8 of the DPDP Act is the operational heart of the statute.[113] It provides that a data fiduciary is responsible for compliance with the Act in respect of any processing undertaken by it or on its behalf by a data processor.[114] In other words, outsourcing processing does not outsource accountability.[115] This has important implications for Indian businesses that rely heavily on cloud service providers, software-as-a-service vendors, outsourced call centres, analytics partners and other third-party processors.[116]

Section 8 requires that processing be limited to lawful purposes and in accordance with the Act, that data be complete, accurate and consistent where it is used to make decisions that affect the data principal or where it is disclosed to another data fiduciary, and that reasonable security

[108] Digital Personal Data Protection Act, 2023, §§ 8, 11–14.
[109] Id. § 15.
[110] Id.
[111] See Digital Personal Data Protection Act, 2023, § 15.
[112] See Vrinda Bhandari & Aman Nahar, Duties of Data Principals Under India's DPDP Act, NLSI-LII Working Paper (2024).
[113] Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 8 (India).
[114] Id. § 8(1).
[115] Id.
[116] See EY, *Decoding the Digital Personal Data Protection Act, 2023* 14–18 (2025) (discussing implications for outsourcing and vendor management).

safeguards be implemented to prevent personal data breaches.[117] The same provision obliges data fiduciaries to notify the Board and affected data principals of a personal data breach in the manner prescribed and to erase personal data once the purpose of processing has been served or consent has been withdrawn, subject to legal retention obligations.[118]

These duties transform data protection into a systems question.[119] A company can no longer rely solely on a general privacy policy drafted by legal counsel; it must design and maintain processes that can demonstrate compliance in practice.[120] That entails maintaining a data inventory, mapping data flows, ensuring purpose limitation, setting up access controls, establishing breach-response protocols, training employees, and integrating privacy considerations into product development and vendor management.[121]

B. Significant Data Fiduciaries and enhanced obligations

The Act recognises that not all data fiduciaries pose the same level of risk.[122] Section 10 empowers the Central Government to notify any data fiduciary or class of fiduciaries as a "Significant Data Fiduciary" based on factors such as the volume and sensitivity of personal data processed, the risk to rights of data principals, the potential impact on sovereignty and integrity of India, the security of the State, public order or electoral democracy, and such other factors as may be prescribed.[123]

Once designated, Significant Data Fiduciaries must comply with additional obligations, including the appointment of a Data Protection Officer based in India, responsible to the Board of Directors or similar governing body; the appointment of an independent data auditor; and the conduct of periodic data protection impact assessments and audits.[124] These measures are intended to embed data governance within the senior management and oversight structures of large or high-risk organisations.[125]

---

[117] Digital Personal Data Protection Act, 2023, § 8(2)–(4).
[118] Id. § 8(5)–(7).
[119] See Kamath & Nahar, Rulemaking for Data Protection: Implementing India's Digital Personal Data Protection Act, 2023, Indian J.L. & Tech. (NLSIU Blog, Apr. 11, 2025) (emphasising systems-level governance under the DPDP Act).
[120] See EY, supra note 116, at 14–19.
[121] Id.; see also GDPR art. 24 (controller responsibility) (comparative reference).
[122] Digital Personal Data Protection Act, 2023, § 10(1).
[123] Id.
[124] Id. § 10(2).
[125] See PRS Legislative Research, *The Digital Personal Data Protection Bill, 2023* – Bill Summary 3–4 (2023)

From a corporate compliance perspective, this tiered approach is sound in principle.[126] It recognises that some entities—large platforms, major financial institutions, health-tech companies, critical infrastructure providers—pose greater systemic risk and therefore require more robust internal governance.[127] At the same time, the breadth of designation factors and the absence of detailed thresholds can create uncertainty for businesses.[128] If designation decisions are not accompanied by clear criteria and transparent reasoning, organisations may struggle to anticipate their obligations or to plan long-term investments in data governance.[129]

C. Sectoral illustrations: finance, health and employment

The implications of the DPDP Act are particularly acute in sectors that already face heavy regulatory oversight.[130]

In finance and fintech, entities must reconcile DPDP obligations with existing requirements under the Reserve Bank of India's cybersecurity directions, outsourcing guidelines, KYC norms and account aggregator framework.[131] Financial institutions are required to retain transaction and customer data for minimum periods for anti-money-laundering and risk-management purposes, while the DPDP Act introduces rights of correction and erasure subject to legal retention.[132] This tension can be managed only through carefully documented retention schedules that distinguish between data kept for legitimate statutory reasons and data that can and should be erased once the purpose is complete.[133]

In health and health-tech, companies handle highly sensitive personal data through telemedicine platforms, online pharmacies, diagnostic apps and health-monitoring wearables.[134] While the DPDP Act does not create a distinct category of "sensitive personal

(explaining heightened obligations for Significant Data Fiduciaries).
[126] Id.
[127] Id.; EY, supra note 116, at 20–21.
[128] See Kamath & Nahar, supra note 119 (noting uncertainty around designation criteria).
[129] Id.
[130] See Reserve Bank of India, Master Direction – Information Technology Framework for the NBFC Sector, RBI/DNBS/2016-17/53, at 1–3 (June 8, 2017); Reserve Bank of India, Cyber Security Framework in Banks, DBS.CO.CSITE/BC.11/33.01.001/2015-16 (June 2, 2016) (illustrating intensive sectoral regulation).
[131] See, e.g., Reserve Bank of India, Master Direction – Know Your Customer (KYC) Direction, 2016 (updated from time to time); Reserve Bank of India, *Circular: Master Directions – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions, 2016* (Sept. 2, 2016).
[132] See Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, r. 3 & r. 9; Digital Personal Data Protection Act, 2023, §§ 12–14.
[133] See EY, supra note 116, at 22–24 (recommending retention policies that align sectoral obligations with DPDP erasure rights).
[134] See National Digital Health Mission, *Health Data Management Policy* (Draft, Aug. 2020) (describing

data" as some earlier drafts proposed, the volume and intimacy of health data clearly influence risk.[135] Health-tech entities must design strong access controls, role-based permissions, encryption practices and strict purpose limitation, particularly to prevent secondary use of health data for discriminatory pricing, employment screening or targeted advertising.[136]

In employment contexts, the Act's legitimate-use provision for employment-related purposes interacts with common corporate practices such as CCTV surveillance, access logs, device monitoring, productivity tracking and vendor background checks.[137] Employers may be tempted to rely on this ground to justify broad monitoring.[138] A proportionality-oriented interpretation would require that any such processing be genuinely necessary, proportionate to the risks addressed, accompanied by clear notice and subject to safeguards against misuse.[139] Otherwise, the workplace risks becoming a near-total surveillance environment under the cover of legitimate use.[140]

VI. Enforcement and Institutional Design

A. The Data Protection Board of India

The DPDP Act establishes the Data Protection Board of India as the central adjudicatory and enforcement body.[141] Section 18 empowers the Board to determine non-compliance with the Act, to direct remedial measures, to accept voluntary undertakings and to impose monetary penalties as provided in the Schedule.[142] The Board is conceived as a "digital office", intended to operate in a technology-enabled manner, receive electronic complaints and conduct inquiries with flexibility and speed.[143]

telemedicine and health-tech data flows).
[135] Compare Personal Data Protection Bill, 2019, § 3(36) (defining "sensitive personal data") with Digital Personal Data Protection Act, 2023, passim (omitting a separate category).
[136] See National Health Authority, *Health Data Management Policy*, supra note 134; OECD, *Recommendation on Health Data Governance* 5–8 (2017).
[137] Digital Personal Data Protection Act, 2023, § 7(f).
[138] See Kamath & Nahar, supra note 119 (warning about broad interpretations of employment-related processing).
[139] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 270–72 (India) (proportionality test); *Modern Dental Coll. & Research Ctr. v. State of M.P.*, (2016) 7 SCC 353, 383–85 (India).
[140] See OECD, *Dark Commercial Patterns* 11–14 (2022) (raising concerns about pervasive monitoring and manipulation in the workplace).
[141] Digital Personal Data Protection Act, 2023, § 18(1).
[142] Id. § 18(2)–(4); Sch.
[143] Id. § 18(1) expl. (referring to a "digital office")

The Board's powers are significant.[144] It can initiate inquiries upon receiving breach notifications, upon references from the Government or other regulators or upon complaints by data principals.[145] It can call for information, conduct hearings, pass interim orders and issue final directions.[146] Penalties for serious contraventions, such as failure to take reasonable security safeguards to prevent data breaches or non-compliance with the obligations of Significant Data Fiduciaries, can reach substantial amounts, potentially running into hundreds of crores, depending on the contravention and the factors considered.[147]

B. Independence, composition and tenure

Despite this enforcement power, the institutional design of the Board raises questions about independence and continuity.[148] The members of the Board are appointed by the Central Government, which also prescribes their terms and conditions of service.[149] Members hold office for a relatively short term and are eligible for re-appointment, subject to age limits.[150] This model is closer to that of an executive authority than to an independent tribunal or regulator.[151]

The Supreme Court's jurisprudence on tribunals and regulatory bodies suggests that mere creation of an ostensibly independent entity is not sufficient.[152] In *Union of India v. Madras Bar Association* and *Rojer Mathew v. South Indian Bank Ltd.*, the Court stressed that adjudicatory bodies exercising important public functions must possess adequate independence from the executive in terms of appointment, tenure, removal and service conditions.[153] While the Data Protection Board is not identical to the tribunals examined in those cases, the underlying principles are relevant.[154] If the same executive that is a major processor and beneficiary of personal data also effectively controls the enforcement body, confidence in

[144] Id. §§ 18, 32–34.
[145] Id. § 18(2).
[146] Id. §§ 18(3), 32–34.
[147] Id. § 33(1)–(2); Sch. items 1–8 (setting maximum penalties up to ₹250 crore for certain contraventions).
[148] See Digital Personal Data Protection Act, 2023, §§ 19–21.
[149] Id. § 19(2)–(3).
[150] Id. § 19(4)–(5).
[151] See PRS Legislative Research, *The Digital Personal Data Protection Bill, 2023* – Bill Summary 4–5 (noting executive control over Board appointments).
[152] See *Union of India v. Madras Bar Ass'n*, (2021) 7 SCC 369, 394–96 (India) (Tribunals Reforms case); *Rojer Mathew v. S. Indian Bank Ltd.*, (2020) 6 SCC 1, 92–99 (India).
[153] *Madras Bar Ass'n*, (2021) 7 SCC 369, 394–96; *Rojer Mathew*, (2020) 6 SCC 1, 92–99.
[154] See *Rojer Mathew*, (2020) 6 SCC 1, 92–99 (emphasising independence of adjudicatory bodies).

impartial adjudication may be weakened.[155]

C. Penalties and remedial philosophy

The DPDP Act's penalty framework is designed to be both flexible and deterrent.[156] The Schedule sets out maximum penalties for different contraventions, and Section 33 requires the Board to consider factors such as the nature, gravity and duration of the breach; the type of personal data affected; whether the breach was repetitive; whether the fiduciary gained a financial benefit; and whether the fiduciary took mitigating measures.[157] This is broadly aligned with global best practice, which emphasises risk-based, proportionate penalties that encourage compliance without necessarily crippling businesses.[158]

The Act does not, however, provide for individual compensation or damages through the Board's process; it is focused on public enforcement rather than private redress.[159] Data principals seeking monetary compensation may have to resort to traditional civil remedies or to sectoral dispute resolution.[160] The absence of a dedicated compensation mechanism could dilute the personal remedial impact of the statute, especially for individuals who suffer tangible harm from data breaches or misuse.[161]

VII. Exemptions, State Power and Constitutional Tension

A. Section 17 exemptions

The most controversial feature of the DPDP Act is its exemption architecture under Section 17.[162] The provision allows the Central Government to notify that certain provisions of the Act shall not apply, or shall apply with modifications, to specific data fiduciaries or classes of fiduciaries for reasons such as the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing

[155] See *Madras Bar Ass'n*, (2021) 7 SCC 369, 394–96; *Rojer Mathew*, (2020) 6 SCC 1, 92–99.
[156] Digital Personal Data Protection Act, 2023, § 33; Sch.
[157] Id. § 33(2).
[158] Cf. GDPR art. 83(1)–(2) (setting criteria for administrative fines); OECD, *Digital Security Risk Management for Economic and Social Prosperity* 12–14 (2015).
[159] See Digital Personal Data Protection Act, 2023, §§ 18, 33 (focusing on public enforcement without a dedicated compensation mechanism).
[160] See id. § 36(1)–(2) (saving other legal remedies).
[161] See Rahul Matthan, Enforcement and Remedies Under India's DPDP Act, 5 Indian L. Rev. (forthcoming)
[162] Digital Personal Data Protection Act, 2023, § 17

incitement to related offences.[163] In addition, various provisions exclude or relax the Act's application in contexts like law-enforcement activities, judicial functions and specified financial processing.[164]

Some of these exemptions may be justified by functional necessity.[165] Law-enforcement agencies cannot always comply with notice and erasure rights while conducting investigations; courts require access to evidence without consent; financial institutions need to process default-related data to protect systemic stability.[166] The problem lies not in the existence of exemptions but in their breadth and in the concentration of exemption-granting power in the executive.[167]

B. Applying proportionality to exemptions

Under *Puttaswamy* and *Modern Dental College*, any limitation on privacy must satisfy proportionality: it must pursue a legitimate aim, be suitable and necessary to achieve that aim, and maintain a fair balance between the aim pursued and the rights restricted, with appropriate safeguards.[168] Section 17 exemptions, if drafted or applied in sweeping terms, risk failing this test.[169] For example, if a broad category of government processing is exempted from core obligations like purpose limitation, data minimisation, security safeguards or breach notification, the proportionality of such an exemption would be highly questionable.[170]

A proportionality-conscious implementation of Section 17 would require that exemptions be narrow, specific, clearly justified and accompanied by alternative safeguards such as internal oversight, external audit, parliamentary reporting or judicial review.[171] General "in public interest" clauses without articulated necessity and proportionality are likely to invite constitutional challenge in the future, especially if coupled with large-scale surveillance or

[163] Id. § 17(2).
[164] See, e.g., id. §§ 3(3), 17(4)–(5), 36 (specific relaxations and savings for court, law-enforcement and financial activities).
[165] See PRS Legislative Research, *The Digital Personal Data Protection Bill, 2023* – Bill Summary 4–5 (identifying law-enforcement and judicial needs for exemptions).
[166] See id.; see also Prevention of Money-Laundering (Maintenance of Records) Rules, 2005; Code of Criminal Procedure, 1973, §§ 91–92 (India).
[167] See Tarunabh Khaitan, Throwing the Delegation Doctrine to the Winds, Verfassungsblog (Dec. 5, 2022) (critiquing broad exemption powers in earlier DPDP drafts).
[168] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, 270–72 (India); *Modern Dental Coll. & Research Ctr. v. State of M.P.*, (2016) 7 SCC 353, 383–85 (India).
[169] See Khaitan, supra note 194.
[170] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 270–72; Digital Personal Data Protection Act, 2023, § 17(2).
[171] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 270–73; *Modern Dental Coll.*, (2016) 7 SCC 353, 383–85

data-sharing programmes.[172]

VIII. Reform Directions and Governance Recommendations

A. Clarifying exemptions and strengthening safeguards

A first reform priority is to clarify and narrow Section 17 exemptions.[173] This could be achieved through amendments specifying that exemptions must be necessary and proportionate to a clearly defined aim, limited in duration and subject to periodic review.[174] The law could require that exemption notifications set out reasons and safeguards, and that they be laid before Parliament for scrutiny.[175] Such measures would align the Act more closely with *Puttaswamy*'s proportionality framework and with comparative standards on state access to data.[176]

B. Enhancing the independence of the Data Protection Board

A second reform area is institutional independence.[177] The appointment and tenure framework for the Data Protection Board could be strengthened by introducing a selection committee with representation from the judiciary and independent experts, by providing security of tenure with limited grounds for removal and by ensuring budgetary autonomy.[178] These changes would not only protect the Board's independence but also increase the credibility of its decisions in the eyes of data principals and data fiduciaries alike.[179]

C. Addressing dark patterns and manipulative design

Another governance priority is to address dark patterns and manipulative interface design.[180] Consent and rights mechanisms can be undermined if users are nudged or steered into choices

[172] See Gautam Bhatia, State Surveillance and the DPDP Act, 6 Indian L. Rev.
[173] See Digital Personal Data Protection Act, 2023, No. 22 of 2023, § 17 (India).
[174] See *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, 270–72 (India) (proportionality test); *Modern Dental Coll. & Research Ctr. v. State of M.P.*, (2016) 7 SCC 353, 383–85 (India) (structured proportionality).
[175] See *In re Delhi Laws Act*, AIR 1951 SC 332 (India); *Avinder Singh v. State of Punjab*, (1979) 1 SCC 137, 144–45 (India) (emphasising legislative responsibility for essential functions).
[176] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 270–73; GDPR arts. 23, 52 (limiting restrictions and guaranteeing supervisory authority independence) (comparative benchmark).
[177] See Digital Personal Data Protection Act, 2023, §§ 18–21 (Board constitution and appointments).
[178] See *Union of India v. Madras Bar Ass'n*, (2021) 7 SCC 369, 394–96 (India); *Rojer Mathew v. S. Indian Bank Ltd.*, (2020) 6 SCC 1, 92–99 (India) (tribunal independence principles).
[179] See PRS Legislative Research, *The Digital Personal Data Protection Bill, 2023* – Bill Summary 4–5 (2023) (raising concerns regarding Board independence).
[180] See OECD, *Dark Commercial Patterns* 11–18 (2022).

that they would not make in a neutral environment.[181] While the DPDP Act does not explicitly address dark patterns, the notions of "free" and "informed" consent, as well as fiduciary duties, can be interpreted to prohibit such practices.[182]

Rules or guidelines could specify examples of prohibited interface designs, such as pre-ticked consent boxes, confusing toggles, hiding of opt-out options, or making privacy-protective choices more burdensome than data-sharing choices.[183] This would ensure that the formal language of consent is matched by genuine autonomy in practice.[184]

D. Coordinating with sectoral regulators and competition authorities

Finally, effective data protection governance requires coordination among regulators. Data protection intersects with financial regulation, health regulation, telecommunication, consumer protection and competition law.[185] For example, data-driven market power and unfair data practices may raise both privacy and competition concerns.[186] Memoranda of understanding, joint working groups and coordinated enforcement strategies between the Data Protection Board, sectoral regulators and the competition authority can prevent fragmented or contradictory regulatory signals.

Such coordination can also facilitate more nuanced remedies.[187] In some cases, structural or behavioural remedies imposed by a competition authority may be reinforced by data protection obligations, while in others, data protection issues may be better addressed through sectoral conduct rules.[188] The DPDP Act's broad aims will be most effectively realised when it functions as part of an integrated regulatory ecosystem.[189]

---

[181] Id.; Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 563–66 (2008).
[182] Digital Personal Data Protection Act, 2023, § 6(1); see also GDPR art. 7(2)–(4) (requirements for consent and prohibition of manipulative consent design) (comparative).
[183] See OECD, supra note 218, at 15–18.
[184] See Barocas & Nissenbaum, Big Data's End Run Around Anonymity and Consent, in *Privacy, Big Data, and the Public Good* 44, 50–52 (Julia Lane et al. eds., Cambridge Univ. Press 2014).
[185] See Digital Personal Data Protection Act, 2023, § 18(4) (coordination with other regulators).
[186] See Competition Act, 2002, No. 12 of 2003, §§ 18–19 (India) (functions of Competition Commission of India); Reserve Bank of India Act, 1934; Telecom Regulatory Authority of India Act, 1997; Consumer Protection Act, 2019.
[187] See Autorité de la concurrence & Bundeskartellamt, supra note 225, at 10–12.
[188] See Competition Comm'n of India, *Market Study on the Telecom Sector in India* 89–93 (2021) (discussing data and competition); Kamath & Nahar, supra note 214.
[189] See Digital Personal Data Protection Act, 2023, pmbl. (integrating rights protection with digital innovation); EY, supra note 215, at 26–28.

IX. Conclusion

The Digital Personal Data Protection Act, 2023 marks a historic step in India's legal response to the realities of a data-driven society.[190] It translates the Supreme Court's recognition of privacy as a fundamental right into a statutory framework that defines roles, responsibilities and remedies in the processing of digital personal data.[191] For corporate India, the Act signals that data protection is no longer a peripheral compliance item; it is a core governance concern that demands attention from boards, senior management, engineers and lawyers alike.[192]

Yet the Act is as much a beginning as it is a culmination.[193] Its brevity, reliance on delegated legislation, modest rights catalogue and broad exemptions make it a framework that requires careful institutional development.[194] The independence and functioning of the Data Protection Board, the quality of rules and guidance, the approach to exemptions and the willingness of corporations to embed privacy into design and culture will together determine whether the DPDP Act realises its constitutional promise.[195]

If implemented with proportionality, transparency and genuine institutional autonomy, the Act can anchor a robust regime of digital accountability and contribute to a broader project of digital constitutionalism in India.[196] If, however, exemptions are used loosely, enforcement is uneven and compliance is reduced to paperwork, the statute may legitimise rather than constrain data exploitation. The choice between these futures will be made not only in courts and ministries, but also in how Indian companies, regulators and citizens internalise the values of privacy, dignity and accountability in the everyday governance of data.[197]

---

[190] See Digital Personal Data Protection Act, 2023, pmbl.; *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 266–67.
[191] Digital Personal Data Protection Act, 2023, §§ 2–4, 8, 11–18.
[192] See EY, *Decoding the Digital Personal Data Protection Act, 2023* 6–8 (2025).
[193] See generally Committee of Experts on Data Protection Framework for India, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* 1–4 (2018); Digital Personal Data Protection Act, 2023, pmbl.
[194] Digital Personal Data Protection Act, 2023, passim; see also PRS Legislative Research, *The Digital Personal Data Protection Bill, 2023* – Bill Summary 2–5.
[195] See *Madras Bar Ass'n*, (2021) 7 SCC 369, 394–96; *Rojer Mathew*, (2020) 6 SCC 1, 92–99; Kamath & Nahar, supra note 214.
[196] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 270–73 (linking privacy, accountability and constitutionalism); OECD, *Digital Security Risk Management for Economic and Social Prosperity* 12–15 (2015).
[197] See *Puttaswamy (Retd.)*, (2017) 10 SCC 1, 193–97 (discussing privacy, dignity and democratic culture).