CONSTITUTIONAL STATUS OF DATA PROTECTION IN INDIA: A CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Akshita Singh, Amity Institute of Advanced Legal Studies, Amity University, Noida

ABSTRACT

This paper examines the constitutional status of data protection in India through a critical analysis of the Digital Personal Data Protection Act, 2023 (DPDP Act). The recognition of the right to privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) marked a decisive shift in Indian constitutional jurisprudence, establishing informational privacy as an essential facet of dignity, liberty, and autonomy under Articles 14, 19, and 21. In response, the DPDP Act seeks to provide a statutory framework governing the processing of digital personal data.

The paper traces the evolution of privacy jurisprudence from early judicial resistance in M.P. Sharma v. Satish Chandra (1954) and Kharak Singh v. State of Uttar Pradesh (1963) to its eventual constitutional affirmation. It evaluates whether the DPDP Act successfully translates constitutional principles into an effective regulatory regime. The analysis identifies key structural and normative concerns, including legislative minimalism, excessive executive discretion, expansive state exemptions, dilution of consent through "legitimate uses," and the limited scope of data principal rights. It also highlights issues relating to the institutional independence of the Data Protection Board, the tension between privacy and transparency following amendments to the Right to Information Act, 2005, and challenges arising from cross-border data flows and algorithmic governance.

The paper argues that while the DPDP Act represents a significant step towards formalising data protection in India, it adopts a predominantly compliance-oriented and executive-driven framework rather than a robust rights-based approach. As a result, it only partially fulfils the constitutional mandate of protecting informational privacy. The study concludes that the effectiveness and constitutional validity of India's data protection regime will ultimately depend on judicial scrutiny, regulatory interpretation, and future legislative refinement.

Keywords: Data Protection, Right to Privacy, Informational privacy, Digital Personal Data Protection Act, 2023, Constitutional Law, Consent and Legitimate Use, Executive Discretion, Cross- Border Data Transfers.

INTRODUCTION

Data protection is a crucial issue in the present era especially due to the technological advancements that have taken place in the past few decades.[1] Not like that data protection is a comparatively latest concept, but modern-day technologies have made it easier to steal and exploit data, making it a much bigger issue now. Misuse of data can have horrendous consequences which is the reason why data protection and privacy are essential topics among the scholars of our Constitution. The constitutional status of data protection in India is rooted in the interpretation of Article 21 which guarantees the right to life and personal liberty. The Supreme Court Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[2], unanimously recognized the right to privacy as a fundamental right u/Art 21[3], as well as an essential component of freedoms guaranteed u/Art 14 and 19[4].

Subsequent judicial pronouncements further strengthened this constitutional foundation. In Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act Case (K.S. Puttaswamy v. Union of India, 2018)[5], the SC emphasized the principles of proportionality, necessity, and legality in any State action involving personal data. Similarly, in Anuradha Bhasin v. Union of India (2020)[6], the Court reiterated that restrictions on fundamental rights in the digital domain must satisfy constitutional tests of reasonableness and proportionality. In response to these constitutional mandates, Parliament enacted the Digital Personal Data Protection Act, 2023.[7]

This article undertakes a critical analysis of the constitutional status of data protection in India with specific reference to the Digital Personal Data Protection Act, 2023. The Act seeks to operationalise informational privacy by regulating the processing of digital personal data, defining the rights of data principals, and imposing obligations on data fiduciaries. While it introduces consent-based processing, accountability mechanisms, and enforcement through the Data Protection Board of India, several provisions raise constitutional concerns. Broad state exemptions, diluted consent standards, limited individual rights, and restricted institutional

[1] Gajjar, N. T. (2024). Data privacy and protection in the digital age: Emerging trends and technologies. International Journal of Engineering Applied Science and Management, 5(4), 1-4.
[2] AIR 2017 SC 4161.
[3] The Constitution of India 1950.
[4] Ibid.
[5] (2017) 10 SCC 1.
[6] AIR 2020 SUPREME COURT 1308.
[7] Saurabh, S. (2024). The Digital Personal Data Protection Act of 2023: Strengthening Privacy in the Digital Age. Int'l JL Changing World, 3, 77.

independence invite scrutiny under the proportionality and reasonableness tests laid down in the relevant case laws. The study evaluates the adequacy, limitations, and future implications of India's evolving data protection regime

HISTORICAL BACKGROUND

In the early decades after independence, the Constitution of India did not explicitly recognize privacy or data protection as a fundamental right. Judicial interpretation during this period focused primarily on physical liberty and procedural safeguards, with limited engagement with informational autonomy.

The first significant judicial engagement with the idea of privacy arose in *M.P. Sharma v. Satish Chandra* (1954)[8], where an eight-judge bench of the Supreme Court rejected the existence of a constitutional right to privacy while examining search and seizure powers under the Code of Criminal Procedure. This position was reiterated in *Kharak Singh v. State of Uttar Pradesh* (1963)[9], in which the Court struck down domiciliary visits but declined to recognize privacy as a fundamental right, confining its protection to personal liberty in a narrow sense. From 1970s onwards, judicial thought began to evolve alongside changes in governance and surveillance practices. In *Gobind v. State of Madhya Pradesh* (1975)[10], the Supreme Court acknowledged privacy as an implicit right under Article 21, though subject to reasonable restrictions. Subsequent cases such as *R. Rajagopal v. State of Tamil Nadu* (1994)[11] and *People's Union for Civil Liberties v. Union of India* (1997)[12] further expanded privacy protections, including informational privacy in context of telephone tapping, indicating judicial awareness of emerging communication technologies.

Parallel to judicial developments, India's technological landscape underwent substantial transformation in the late 1990s and early 2000s. The liberalization of the economy and the growth of the information technology sector necessitated legal recognition of electronic records and digital transactions. This led to the enactment of the Information Technology Act, 2000, India's first legislation addressing electronic data. While the Act primarily focused on cybercrime and e-commerce, Section 43A, introduced through the 2008 amendment, imposed

[8] AIR 1954 SUPREME COURT 300.
[9] 1964 SCR (1) 332.
[10] AIR 1975 SUPREME COURT 1378.
[11] 1994 SCC (6) 632.
[12] AIR 1997 SC 568.

compensation liability on body corporates for failure to protect sensitive personal data. The accompanying Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, constituted India's earliest statutory attempt at data protection, albeit limited in scope and applicability.[13]

A decisive shift occurred with the launch of Aadhaar project in 2009, which involved large-scale collection of biometric and demographic data.[14] The constitutional challenges to Aadhaar foregrounded concerns regarding surveillance, consent, and informational privacy, ultimately catalyzing a comprehensive judicial reconsideration of privacy. This culminated in the landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), where a nine-judge bench unanimously overruled *M.P. Sharma* and *Kharak Singh*, affirming privacy as a fundamental right under Articles 14, 19, and 21.

In response, the Government constituted the Justice B.N. Srikrishna Committee in 2017 to examine issues relating to data protection. The Committee's 2018 report, titled "A Free and Fair Digital Economy," proposed the Personal Data Protection Bill, 2018, grounded in principles of consent, purpose limitation, data minimisation, and accountability. The Bill underwent revisions and was introduced as the Personal Data Protection Bill, 2019, incorporating expanded State exemptions and revised regulatory mechanisms.[15]

Continued deliberations led to the withdrawal of the 2019 Bill in 2022, followed by the introduction of the Digital Personal Data Protection Bill, 2022, reflecting a shift towards a simplified, principle-based framework. This legislative process culminated in the enactment of the Digital Personal Data Protection Act, 2023. The Act represents the latest stage in India's data protection evolution, emerging from decades of constitutional interpretation, technological change, and policy experimentation.

CRITICAL EVALUATION AND CHALLENGES

The Digital Personal Data Protection Act, 2023 (DPDP Act) may be India's first attempt to align with the constitutional requirement of a modern privacy law. In a broad sense, this

[13] Kashyap, A. K., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. Law & Safety, 207.
[14] Bhatia, A., & Bhabha, J. (2017). India's Aadhaar scheme and the promise of inclusive social protection. Oxford Development Studies, 45(1), 64-79.
[15] Burman, A. (2022). Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?. Carnegie Endowment for International Peace.

description suffices to justify the significance of the Act, considering the extent of the shift from the absence of a statute focused on digital personal data to now having a statute on the subject. However, the point that remains to be made is the extent of the significance, as opposed to the absence of significance. With respect to the statute that was legislated post Justice K.S. Puttaswamy (Retd.) v. Union of India, it is inadequate to simply create a compliance regime. Such a statute should be able to embody a constitutional perspective on privacy that is socio-economically oriented towards dignity, autonomy, equality, and accountability. It is this critical challenge that this chapter undertakes, to identify the gaps in the DPDP Act, particularly in the design, and in the likely operationalisation of the Act, as well as to determine the effect of such gaps being the result of choices of drafting, or structural factors that will, to a greater extent, be determinative of the extent to which the privacy of the Digital Constitution of India would be compromised.[16]

It is a limited, but foundational, privacy statute to be based on the DPDP Act. The central point of this chapter is that the gaps are not simply isolated drafting errors. Issues in the very design of the law must be identified by the way broad executive discretion, wide exemptions for the State, a narrow scope of user rights, little independence for regulators, too much reliance on delegated legislation, as well as a compliance rather than rights approach to enforcement. These issues have long since moved beyond the classroom. After the criticism of the draft Act and the Digital Personal Data Protection Rules of 2025 by civil society, policy analysts, and legal scholars, the documents' phased operationalisation on the 11th of November 2025 have commenced. Challenges to the various components of the DPDP framework, particularly the revision of the Right to Information Act, have reached the Supreme Court. In February 2026, the Supreme Court declined to stay the Act and referred the case to a larger bench.[17]

There are, however, two dimensions to a full critique of the Act. First, is this legislation theoretically consistent with constitutional privacy jurisprudence and the best practices globally? Secondly, and perhaps more importantly, in the face of India’s exponentially growing digital ecosystem, is the legislation likely to offer sufficient protection to the average user, as they encounter and interact with banking and telecom services, e-commerce, health apps, social media, education, employment, welfare and public and various other databases?

[16] Supra note 66.
[17] Supra note 66.

The importance of the digital divide in India is particularly relevant because the digital divide impacts how people access rights, services, market transactions, and digital identities. Therefore, data protection legislation is not a purely technical issue. It is a constitutional issue of the technology of power.

The momentum of a constitutional critique of the Act is consistent with the critique of the fracturing of the executive's control of the data protection framework; the scope and scale of State-giving exceptions; the weakening of consent as the basis for lawful data processing; the procedural and institutional deficits; the ambiguity of board's power and enforcement; the contradictory provisions of privacy and transparency in the amended RTI Act; the inadequacy of protections for children and other vulnerable persons; the inadequacy of privacy and grievance mechanisms for data subjects; the insufficient mechanisms for control of the trans-border flow of data; and the insufficiency of provisions in the Act to address the data protection issues in a highly datafied economy characterised by asymmetric, large-scale, and opaque issues. The chapter aims to provide a comprehensive critique of the constitutional and regulatory framework through an evaluation of the Act, the suite of rules and guidelines expected to be developed in 2025, relevant case law, academic and policy papers, and the body of public commentary.[18]

I. The DPDP Act as a Minimalist Privacy Statute

The DPDP Act demonstrates extreme legislative minimalism. Not only is the Act consistent in this approach, it leaves most details to be filled in by more executive prescriptions, and standard privacy principles and rights are omitted completely. This might have shielded the legislators from complex administration or drawn-out descriptions like those contained in the discarded Personal Data Protection Bill, 2019. However, brevity is not a virtue when applied to privacy legislation. Where the law regulates the exercise of a fundamental right that necessitates the careful structuring of legal power between the state and the large private entities, underspecification often leads to discretionary governance instead of a reigns-based approach.

The statute provides great protections, but it is not constructed on a robust system of principles like the GDPR. In fact, it is the absence of a single, comprehensive general provision that constitutes the law’s integral framework of principles like legality, fairness, transparency,

[18] Arundhati, M. A. (2025). Data Protection and Regulation: New Avenues for India-EU Cooperation. In Contours of India-EU Engagements (pp. 99-121). Routledge.

purpose limitation, data minimisation, storage limitation, integrity, confidentiality, accountability, and lawfulness that creates the absence of a principles clause. These ideas do emerge, albeit in a scattered fashion, through sections on notice and consent, breach notification, accuracy, erasure, and significant data fiduciaries. However, the absence of a principles clause creates articulated ideas in law with real consequences.[19]

They aid developers in providing interpretive guidance, setting limiters on discretion, and assist regulators and adjudicators in addressing unanticipated issues and/or problems in a rights-protective policy manner. If these principles are vaguer, then the more the power shifts towards executive interpretation and compliance formalism.[20]

The rights catalogue also shows the same minimalistic pattern. The Act provides data principals rights of access, correction, erasure (in some situations), grievance redressal, and nomination. However, it excludes a number of rights present in more robust privacy regimes such as the right to object to processing, the right to data portability, the right to limit processing, and the right to be free from significant automated decision making. The absence of these rights protection in a ranking economy, recommendations, and automated verification, targeted persuasion, and machine-generated risk scores, is deliberate. This indicates a shift towards a more administrative, transactional approach, rather than one that overwhelmingly centres on self-determination. This minimalistic approach can create the appearance of stability. The Act's design is, at least superficially, clean and modern. Yet in reality, its compact structure simplifies and avoids more complex questions, shifting them to rules, notifications, sectoral guidance, Board practice, and litigation. This approach ultimately allows Constitutional questions to not be addressed by the Parliament.

Puttaswamy views this as a serious concern, as privacy limitations should rest legally, with the requisite precision and safeguards, as opposed to broad statutory frameworks with gaps to be filled by subsequent executive actions.

II. Executive Discretion as a Structural Problem

The Central Government's monopolisation of power is the most essential theoretical and practical concern regarding the DPDP framework. The role of the executive under the Act is

[19] Supra note 71
[20] Supra note 71

more than being an implementing authority; they are also a conceptual co-builder of the Act's practical content. The executive decides when the Act is implemented, develops the regulations, publishes a list of the destinations of restricted transfers, identifies significant data fiduciaries, establishes criteria for the exercise of certain discretionary powers, creates categories for exemptions, and controls the majority of the design of the institution of the Board. The executive can also request information under the Rules for a number of state-related purposes. The amount of control the executive has raises a fundamental constitutional question. Given the amount of control the executive has in designing enforcement and exemptions, can privacy legislation be considered protective of rights?[21]

The concern is very real. The phased commencement notification issued on 13 November 2025 is a case in point showing just how much operational content of the law is dependent on the Executive's discretion. The Government's Rules of 13 November 2025 also follow the same pattern. Some of the provisions themselves became operational immediately, some became operational after one year, and the core functional provisions after a period of eighteen months. This indicates that the executive not only controls the interpretation of the Act via rulemaking, but also controls the tempo at which rights and duties become real in the context of the regulation. While this kind of temporal discretion may be administratively convenient, it implies that the operational lifespan of privacy rights is contingent upon the executive's ordering rather than solely upon the statute as passed.

The scope of delegated legislation is also noteworthy; a number of central issues are left to the rules: notice templates, the obligations of a consent manager, breach reporting templates, parental consent verification, state-linked processing, Board functioning, compliance obligations of significant data fiduciaries, and the ways in which the Central Government may regulate information from fiduciaries and intermediaries. While such delegation may be commonplace in an everyday regulatory environment, in a context that concerns a constitutionally protected right, this sort of delegation becomes constitutionally substantial. Each time Parliament chooses not to decide an issue, an increasing amount of the practical scope of the right to privacy is placed at the discretion of the executive in the manner of policy rather than in the legislative act that is subject to sufficient democratic deliberation.

[21] Yadav, A., & Pandey, R. (2025). Data Privacy across Borders: A Comparative Analysis of European Union and Indian Protection Laws. U. Bologna L. Rev., 10, 177.

This is the concern reflected in the civil society response to the draft rules from 2025. The Centre for Internet and Society has argued that some of the Rules seem to move the cross-border transfer model further than what the Act contemplates, and that the legislative "negative list" structure seems to have been converted into something more controlled or altered by subordinate legislation. While the exact legality of that comment would likely require some form of adjudication, the comment does capture the predominant concern: if the statute is open-textured and the executive has wide-ranging authority, then subordinate norms can adjust the balance of rights in ways that are not apparent from the statute in question.[22]

There is also an effect on the structure of accountability that is executive-centric and more subtle; if a privacy statute is to be ideal, then power should be distributed among Parliament, an independent regulator, the courts, and the public. However, the DPDP framework frequently redistributes power to the Union executive. This may enhance administrative coherence, but it also increases the risk of a dilution of rights under political pressure, security anxiety, bureaucratic convenience, or developmental urgency. In constitutional democracies, the very moments when state interests can be invoked most readily are when privacy rights are most under threat. A rights-protective law should not entrench that tendency, but rather anticipate it.

III. State Exemptions and the Constitutional Tension with *Puttaswamy*

Most critics of the DPDP Act are not satisfied with the Act's state-related carve-outs. Section 17 of the DPDP Act allows major classes of processing to exempt themselves from core obligations and the rights chapter. Furthermore, it allows the Central Government to exempt any instrumentality of the state or any class thereof in the interest of the sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or to prevent incitement to a cognisable offence, as the case may be. The question here is not whether any such interest is legitimate. They obviously can be. The question is whether the statute cabins such exemptions enough to pass the constitutional tests of necessity, proportionality, and some sort of procedural safeguards.

Puttaswamy's analysis of privacy points to the need for restrictions on the privacy of individuals to be lawful, to serve a legitimate purpose, and to be necessary and proportionate, with safeguards against abuse. Consequently, a statute that essentially empowers the executive

[22] Supra note 74.

to carve out large sections of state processing from the usual data protection obligations is, in principle, to provide a detailed justification for why it is outside the ordinary obligations, what narrower options are available, the scope of monitoring with respect to the exemption, and available remedies. The DPDP Act does not do this adequately.[23]

Section 17 is broadly structured, uses expansive terms, and features a thin layer of independent review. This makes it difficult to see how one could argue that the exemption design is constitutionally defensible. The practical ramifications of this structure become clearer when read alongside the 2025 Rules. Rule 5 allows state and state instrumentality processing of personal data for the issuance and provision of subsidies, benefits, services, certificates, licences, or permits, and to process this data per the provisions of the Second Schedule. The Rules provide a framework whereby the Central Government can, for certain state purposes outlined in the Seventh Schedule, direct data fiduciaries or intermediaries to provide data. These purposes include the State or its instrumentalities' use of personal data in the interests of the sovereignty and integrity of India or the security of the State, including under the law. Such provisions suggest that access and processing linked to the State continues to be intertwined in the framework, more often than not through rules and schedules, rather than a more direct statutory approach.

The constitutional concerns do not stem from the fact that the State has legitimate concerns for security, welfare, law enforcement, and administration. Modern governance inevitably means that the State will process data.

The issue at hand is that the Act provides the State with considerable latitude to operate outside the ordinary rights-and-obligations matrix while offering scant legal guarantees that such processing will be truly necessary and proportionate. This absence of legal safeguards is especially troubling when placed in the context of a legal system in which India does not have a general, comprehensive reform statute on surveillance and where numerous data-intensive administrative systems that have a massive scale of operation. Given this situation, one may contend that there is a prima facie case for the broad exclusion clause; however, in point of fact, that may not be the case.[24]

The exemptions for research, archiving, and statistics have similar issues. These types of

[23] Supra note 74.
[24] Supra note 74.

exemptions are often seen in legislation around the world, and there is often a case for them. However, when legislation is silent on the meaning of legitimate research, and there are no robust anonymisation and minimisation requirements, the exemption effectively provides a very large, and very poorly controlled erosion of the law's purposes. The Internet Freedom Foundation noted in its comments on the draft rules that the research exemption did not specify who could invoke it, what research was legitimate, and did not require the consent of data principals. This criticism encapsulates the larger issue: in the absence of an adequate legal framework, abusive processing of personal data is highly likely to occur, especially when the purposes of the data collection are vague. Similar concerns may be raised with regard to relaxations specific to startups or certain categories of startups.

It may make economic sense to relax compliance burdens for small entities. However, if exemptions are crafted too broadly, they could inadvertently create a privacy gradient whereby individuals are protected to differing extents based on the type of commerce or stage of business growth of the entity collecting their data. The protection of fundamental rights should not be so heavily dependent on the thinking of industrial policy. A balanced approach would be to fine-tune compliance mechanisms and not erode the essence of core rights.

IV. Dilution of Consent and the Rise of “Legitimate Uses”

The DPDP Act places consent at the centre of its design. In Section 6, the Act states that consent must be free, specific, informed, unconditional, unambiguous, and given through a clear affirmative action. Not only are these requirements strong, but they are also some of the most defensible features of the Act. However, the positioning of consent in the statute is not as central as it appears. This is due to Section 7 of the Act, which contains a broad range of "certain legitimate uses" that allow for the processing of personal data without consent. These include information volunteered by the data provider, some functions of the State, compliance with legal obligations, medical emergencies, public health, disaster response, and employment. No privacy statute should rely solely on consent. This is well established. Data relationships are far too complex and a large number of processing scenarios cannot be realistically consent-driven. This is the problem with the DPDP Act's broad legitimate use category. It is broad enough to remove the need for consent in a large number of everyday scenarios. When that is the case, the formal strength of Section 6 is significantly diminished. The DPDP Act is a statute designed to promote meaningful consent, but in practice, it will permit a host of processing

activities to occur without consent.[25]

Here we see one of the key theoretical tensions of the Act: the symbolic model is user choice, but the operational model is, more often than not, statutory authorisation. An illustrative example is the voluntary-provision clause. It enables purpose-bound processing of personal data provided by the data principal voluntarily and in the absence of an opt-out indication. This kind of formulation is more operationalisable than a fully-fledged consent workflow, but it is equally risky as it may establish a precedent for normalising implied consent in situations where users provide data for transactional, informational, or participatory purposes—not because they voluntarily consented to a broad data processing paradigm. In the absence of genuine consent, silence, context, or ordinary use can suffice. In an unbalanced and ill-structured market, such a provision can greatly erode the individual's control.

Concerns arise from the employment-related legitimate use as well. In an employment context, for instance, processing personal data without consent may be justified for loss or liability safeguarding purposes, including countering corporate espionage and safeguarding trade secrets. While some such processing is obviously necessary in employment relationships, consent is the least meaningful in such relationships because of the structural power imbalance.

In a more developed version of the DPDP Act, the Act would require heightened fairness, necessity, and transparency duties when it comes to employment. Instead, the DPDP Act resolves the problem of employee data processing by moving the processing outside of employee consent, and shifting the problem without creating a substitute framework of worker-data protections. There is a privacy shift from autonomy to managerial privacy. Protective agency is only provided when the entity processes user data. For data processing, the responsive agency is not provided. The ‘notice and choice’ framework is almost irrelevant for consent fatigue, dark patterns, multilingual interfaces, user literacy gaps, and platform dependence. There is a negative predilection for the user. If the routing for processing data without consent is broad, the user agency is far less than the regulation provides.[26]

V. Consent in Practice: Form, Fatigue, and Informational Asymmetry

Securing the theoretical form of consent is still greatly impractical because of the challenges

[25] Mukherjee, S. Genomes, Consent, and the Law: Navigating the DPDP Act, 2023 and Global Standards. IJAIDR-Journal of Advances in Developmental Research, 16(2).
[26] Supra note 78.

of the Indian regulatory framework. Section 6 elaborates on the quality of consent, with the Rules stating that all notices must be clear, standalone, and available in the English language or any language of the Eighth Schedule. Although these additions to the framework are positive, the gap between formal validity and substantive understanding is still great. In the actual digital marketplace, the user is faced with terms of service, interface nudges, preconfigured ecosystems, bundled services, time pressure, and the user has very little control. The law can state that consent must be free and informed, and still, if the regulators do not act to remedy the situation, the result will be a lack of meaningful choice.

The scale and diversity of India's digital economy also amplifies this problem. Millions of users are impacted by low-cost smartphones, distributed devices, apps in local languages, digital points of assistance, and compulsory or quasi-compulsory digital entrances to services. In this context, the right to informational self-determination is often circumvented by economic urgency rather than by rational choice. A person may consent to the processing of data because no welfare access would be possible if they refuse, and the same goes for employment, credit, or digital life in general. In this scenario, a more complex set of questions arise than simply determining whether the consent form placed in a proper manner is possible to compel the individual to consent to something without undue adverse consequences to the individual. It would seem that the DPDP Act sidesteps this structural dimension of consent.[27]

The issue of withdrawal reaches a similar conclusion. Section 6 of the Act states that withdrawal must be as easy as giving consent. In theory, this is correct. However, most data ecosystems are constructed on many layers of multiple processors, vendor networks, identity providers, advertising, and analytics services. In order for withdrawal to be meaningful, even in that context, the user must be able to pinpoint the destination of the data after it was collected, what processing will be done to the data after the collection under some other alternate legal bases, and how to stop or verify the data processing. The Act fails to provide the user adequate means to access other processing logs, data portability, or a right to withdraw which could have provided a more meaningful and operative dimension to the withdrawal right. Therefore, a user can withdraw consent but has no means to determine or control the actual downstream consequences of the withdrawal right.

Part of the problem of consent has been addressed by consent managers. In principle, they

[27] Supra note 78.

could provide an additional layer of sophistication to the user to provide, review, manage and withdraw consent in an interoperable system. While this enhancement is to be welcomed, consent managers have been given their own set of additional challenges. The consent manager now becomes an additional intermediary of trust and power.

Their effectiveness hinges on true neutrality, operational interoperability, user understanding, and the avoidance of being captured by the fiduciaries whose consent flows they mediate. Absent such conditions, consent managers could be yet another layer of compliance that enhances dashboards without redistributing control. The Act and Rules institutionalise, but whether they will be liberating or simply decorative is still an open question.

VI. Limited Institutional Independence of the Data Protection Board

Implementing regulations and their enforcement hinge on the strength of the enforcement agency. The DPDP Act creates the Data Protection Board of India and states that it is to be independent. However, reading the statutory provisions indicates a lack of institutional independence and fragility. The Central Government has control over the Board composition by virtue of appointing the Chairperson and members, establishing their remuneration and other service conditions, determining where the headquarters is located, and obtaining approval of all staff. The tenure of the Members is two years and is a bar to reappointment. A short tenure proscribed by reappointment creates a relational dependency where reappointment is within the discretion of the executive.

The Board is going to be responsible for adjudicating disputes with the state and large, well-resourced private sector actors. A regulator with these institutional design features is likely to find it harder to take politically sensitive decisions. In these situations, the problem is not the Board's stated incompetence, but rather the design that lacks the components that could be assumed to exist. In privacy regulation, the design and also the functionality matter.[28]

The structural independence of the enforcement agency from the regulating executive branch is a precondition for the public to trust the enforcement agency. Positive portrayals in the Rules and other official texts about the Board do not relieve structural apprehensions. PIB branding casts the Board as an independent body with broad enforcement powers concerning compliance

[28] Hijmans, H. (2006). European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority, The. Common Market L. Rev., 43, 1313.

and enforcement. Such portrayals do not alleviate the apprehension. In contrast, the GDPR, and other global privacy regulations, more fully articulate the independence and separation of oversight functions. The difference is not merely cosmetic. It is a reflection of the understanding that the institutional proximity of privacy/data protection regulators to the executive branches of government is not tenable.

The Board's authorizations further compliance-centric powers. The Board is given authorizations to provide remedial directives, undertake enforcement actions, issue compliance directives, and impose penalties. While these powers are significant, the other components of the Act emphasize breach responses and set procedural limits to other normative oversight of the Act's provisions on fairness, algorithmic harm, or other systemic sectoral abuse. While the acceptance of voluntary commitments can be efficient, it can also lead to a situation of negotiated compliance in the absence of decision-making by the Board.[29]

In some regulatory areas, this has benefits. However, in privacy law, there is a concern that excessive reliance on settlements and undertakings might hinder the development of public precedent and opaque jurisprudence. The Board's digital-office model is yet another example of demerits mixed with some promise. Digital functioning can enhance reach and efficiency in large countries. However, accessibility is more than just online filing. It encompasses language and legal user support, a user-friendly interface, transparency in decision publishing, and adequate technical support. In the absence of these, digitisation is likely to leave deeper asymmetries unsolved whilst streamlining the process. Many resource and literacy-constrained users may still find a digitally designed complaint mechanism system very challenging to use.

VII. Grievance Redressal and the Burden on Data Principals

A consistent practical critique of privacy law is that it often focuses or over-focuses a great deal of burden on the individual. In this regard, the DPDP Act is likely no different. In this respect, section 13 states that the data principal has a right of grievance redressal against a data fiduciary or a consent manager, and has to exhaust that opportunity before coming to the Board. Considering that she is one of only a few, it is understandable that the Board is not overly interested and that every grievance does not have to be an enforcement action. But is it fair that the answer involves engaging with the problem? For sophisticated users with bargaining power,

[29] Schütz, P. (2012). Accountability and Independence of Data Protection Authorities—A Trade-Off?. In Managing Privacy through Accountability (pp. 233-260). London: Palgrave Macmillan UK.

this may be manageable. For ordinary individuals dealing with large corporations or public systems, it can be very intimidating, systemically slow, and opaque.

The problem is greater than the inconvenience of having to act in a certain way (i.e. having to interact with the entities that she is engaging with to solve the problem). Empirical scholarly research on the problem illustrates that ignorance of the problem is problematic, including its reticence and trepidation. A data principal may not know the cause of the denial, leak, unwanted targeting, or disruption of the service. She may not know what system, which fiduciary or processor is responsible, what data was used, or whether the processing was on the basis of consent, legitimate use, or on some other basis.[30]

Technically speaking, the ability to file a complaint with the relevant fiduciary and to pursue steps further may be seen as a means to exercise one's rights, but this means these rights may be impractically accessible. This is a way that the law does not fully capture the lack of understanding that comes with digital processing.

The duties of data principals worsen this worry. Duties like not making false or vexatious complaints may seem unobjectionable, but when users are already in a state of uncertainty about the situation, these duties can stifle the legitimate exercise of one's rights. A complainant may decide not to file a complaint, and this could happen simply because they are not completely sure that their suspicion is actionable. In the context of privacy law, the need to deter vexatious complaints must be balanced with the need to keep, and especially, to promote, accessible and unobstructed channels for complaints to be made. If complainants, and especially the general public, do not feel able to approach the system for redress without the fear of being sanctioned, this will not be a system that encourages rights.

A different but related issue is what can be termed as the "depth of remedies". The Board may impose sanctions, but as against the individual or as collective redress, the Act is not as rich as far as individual compensation is concerned. This is significant since privacy harms are a result of one too many, and they are cumulatively and individually trivial but socially very serious. When individual accountability is absent, the systemic accountability is predominantly dependent on the will and the capacity of the regulator. Users may have formal entitlements that are legally defensible, but practically speaking, they possess a minimal degree of

[30] Naithani, P. (2025). Analysis of India's digital personal data protection act, 2023. International Journal of Law and Management, 67(5), 543-553.

enforceable control.

VIII. Ambiguities in Board Powers and Regulatory Authority

An additional issue concerns the lack of clarity around the boundaries of regulatory authority. The Board has the authority to inquire, direct, and impose penalties, and it may act on breach notices, complaints, referrals, or directives. However, the statute often fails to delineate the boundaries of various forms of regulatory actions. The breadth of the inquiry may be extensive, but the mandate is likely to be limited. The degree of the Board's discretion to set standards through guidance is not as elaborated as other more developed regulatory frameworks. This creates uncertainty for both fiduciaries as well as the users.[31]

In some instances, ambiguity can allow for responsive enforcement. However, in the context of the DPDP, ambiguity, when combined with executive control, can be problematic and result in unfavourable outcomes. Extreme regulatory control of the Board's discretion with respect to procedures, interpretation, and frameworks may result in the ambiguity being resolved through overly prescriptive, top-down administrative control, rather than through the exercise of independent, bottom-up, legislative or judicial processes. This is particularly true for emerging issues related to inferential data, standards of anonymisation, harms of profiling, AI-driven decision-making, data-sharing chains, and the compromising of cybersecurity and privacy. The breadth of the Act's drafting does not address these emerging issues, which creates uncertainty about who may regulate these issues. The ability of the Board to accept voluntary undertakings, which may carry potential upside, also presents potential downside risk. Since they also allow greater flexibility in compliance approaches, without the need for the jam of the contested questions in the public domain, they could provide greater rapidity in the resolution of compliance issues. Civil privacy law, for instance, benefits from the authoritative guidance because they explain the compliance requirements to the entire marketplace and, in doing so, contribute to the emerging public jurisprudence of equitable and proportional regulation. When enforcement through settlements occurs too frequently, the system can become administratively overactive while the relevant doctrine lags behind.

Beyond these issues, there is also the matter of how other regulators will interact. In India's already complex digital ecosystem, sectoral bodies for telecom, finance, health, consumer

[31] Gupta, N., & George, A. (2024). Digital Personal Data Protection Act, 2023: Charting the Future of India's Data Regulation. In Data Governance and the Digital Economy in Asia (pp. 34-53). Routledge.

protection, competition, cybersecurity, and platform regulation co-exist. The DPDP Act does not clarify how privacy oversight will work alongside these overlapping areas of regulation. In theory, coordination can be built over time. In practice, however, the absence of clear jurisdictions can stagnate enforcement, create forum shopping (i.e. unregulated spaces), and allow detrimental behaviour to slip through the cracks between regulatory silos. A strong privacy law should not rely on future adjustments to answer such critical foundational questions.

IX.The RTI Amendment and the Privacy-Transparency Conflict

One of the primary discussions regarding the DPDP Act is not in the central principles of privacy, but in section 44, which modifies Section 8(1)(j) of the Right to Information Act. The modification simplifies the previous wording with the newer clause, which states that it will not apply to "information which relates to personal information". The previous RTI provision was much more complex, as it considered unwarranted invasion of privacy and a larger public-interest override. Critics have said the amendment oversimplifies, and extends the bounds, of secrecy too far.[32]

This is a critically important issue as the constructs of privacy and transparency, while distinctly different, are not oppositely placed in a constitutional framework. While privacy ensures a protection of dignity, and autonomy, transparency ensures democratic accountability and the oversight of the public. A mature legal framework should strike a balance to these principles, especially when dealing with personal information of public employees, the use of public funds, state actions, or matters of public concern. An overly broad privacy exemption can protect wrongdoing as much as an overly restrictive privacy law can expose individuals. The real issue is not which value has supremacy in the abstract, but rather, whether the legal test has a balancing function.

The dispute has advanced to a stage where it has become the subject of formal legal proceedings. In February 2026, the Supreme Court decided to put stays on parts of the DPDP framework alongside the amendment to the RTI act and referred existing pleas to a bigger bench. As per reports, petitioners argued that the amendments have instituted a near-complete bar on the disclosure of personal information, whereas previously, the release of information

[32] Yagnik, S. R. (2020). Right to Information:: Constitutional Analyzis. Journal of Constitutional Law and Jurisprudence, 3(2), 8-12.

was justified if the public interest demand warranted it. This ongoing litigation itself demonstrates that the concerns aren't marginal. It gets to the core of the issue of how India manages the reconciling of the two concepts of privacy and democratic accountability.[33]

The posited theory of the Indian data protection discourse is that the amendment to the RTI reveals the possibility that the language of privacy is used as a cloak of invisibility. When the state is able to control the imposition of limits or exemptions to the privacy law as well as control the scaling down of obligations to disclose information under the law on transparency, the chilling effect is to remove public decision making from the reach of scrutiny. This is the concern that a right-respecting privacy framework ought to address. It must preserve the possibility of context-sensitive public interest considerations, and ought not to be replaced by a silence.

X. Cross-Border Transfers and Global Data Flows

Section 16 of the Act adopts a relatively liberal model of cross-border transfer by stating that a transfer is permitted unless the Central Government imposes specific country/territory-based restrictions. This model of negative listing is more straightforward than the multiple layers of the GDPR[34]. From the perspective of digital commerce and global service integration, it is likely more appealing. However, this simplicity comes at the expense of the statute not requiring more elaborate unilaterally restrictive/bottom-line geographically based rights, not reliant on the statutes themselves, or cross-border rights based transfer mechanisms regarding the availability/deferral, onward transfer, or the right to effective recourse/equal protection.

This gap is significant because, in terms of privacy, harm is not confined by borders. When data is exported into transnational systems, individuals encounter increasing difficulties in data location, applicable laws, ongoing data sharing, and available legal remedies. A transfer regime primarily based on executive discretion, rather than legal rights, is devoid of substantive legal principle. It treats cross-border data flow as a political means rather than a fundamental constitutional framework. The critique of the CIS concerning the 2025 Rules raised concerns that the Rules could fundamentally alter the transfer logic in ways that are not fully apparent in the Act. Regardless of whether courts align with the "ultra vires" argument, this situation reveals a weak reliance on rule frameworks for cross-border governance. Given the global and

[33] Supra note 85.
[34] Burman, A. (2019). Will a GDPR-style data protection law work for India. Policy Commons, 15.

ever-evolving nature of the data economy, governance of transfers incorporates both the need for flexible frameworks and the need for defined rights. The flexible framework of the current model may offer the most, but the latter remains insufficient.[35]

This is particularly true within the transnational nature of the core platforms, processors, and cloud infrastructures within India's digital ecosystem. The fragmentation of data across multiple jurisdictions, vendors, and contractual chains makes domestic privacy rights challenging to enforce. The absence of a more sophisticated statutory scheme for privacy rights, extending beyond the borders of India, based on executive policy and contractual design, would be preferable to a rights-averse transfer framework.

XI. Challenges in the Digital Marketplace: Platforms, Profiling, and Inference

The DPDP Act centres around 'personal data' but the evolving digital economy operates not just on disclosed data, but also inferred data, derived data, and model-generated data. Platforms also create user profiles to predict preferences, rank trust, personalise, set pricing, and improve engagement. Many harms result not from the disclosed known data but from the data derived from inference, aggregation, and analytics. Modern privacy laws, to be comprehensive, will need to address, in addition to collection and sharing, the ability to infer, classify, and manipulate. The DPDP Act attempts to do this, but only in part.

This creates a theoretical gap between privacy as control over data and privacy as control over powers. The Act is more suited to regulating the collection, notice, consent, breach, and correction of data than it is to analysing the recommendation systems, ranking systems, and systems of inferential judgement operating in the background. Users are powerless to contest data-driven outcomes, even when those outcomes are highly detrimental. This is particularly true because the Act does not grant users the right to challenge a significant automated decision, nor a right to object to processing—which also serves to deny users the right to contest data-driven outcomes. As such, this implies that when laws are being constructed, they may be the most protective against harms to privacy that are statutorily traditional, and the least protective against the sorts of algorithmic forms of control that are currently central to digital governance and the exercise of power by platforms.[36]

[35] Supra note 87.
[36] Supra note 87.

This problem is not only stemming from India, but given the speed of digitalisation, especially with the rapid development of systems in financial inclusion, employment, education, and social media, this is particularly problematic. Without knowing how a decision is made, users can be effectively profiled in a way that determines whom they can engage with, what they can do, and what level of visibility or credibility they possess. Privacy laws in such contexts, that lack robust mechanisms to challenge or explain opaque decision-making, may offer protection against some superficial violations while leaving the more protective, backend issues unaddressed.[37]

XII. Children, Vulnerable Users, and Digital Welfare

The child-protection provisions of the Act are arguably stronger than the rest of the provisions of the Act. The Act requires that a parent establish verifiable consent and also prohibits tracking, behavioural monitoring, and targeted advertising to children. However, even in this one area that is stronger than the rest of the Act, there is still a lot of complexity to implementation. The requirement of verifiable parental consent means that there is some way in which that identity, or authority, is verified, which itself may include the processing of other data. If these systems are cumbersome or intrusive, then the effort to protect children may create additional privacy burdens.

The question of adolescent autonomy also complicates the matter. The statute applies a child threshold of under eighteen, which is a bright-line approach. While that may be protective, in the context of education, health, and the use of technology, it may be too broad, especially when older minors have the ability to meaningfully exercise autonomy. The Act also addresses this, albeit indirectly, by providing potential executive relaxation for fiduciaries who verifiably safely process children's data. Yet again, this shifts important normative decisions to delegated authority, failing to incorporate a framework of rights beyond the minimum into the statute.[38]

Age is just one way to consider vulnerability. In the context of digital India, the vulnerability that comes with age is compounded by disability, lack of digital literacy, poverty, language, dependence on the support of the government through welfare schemes, informal employment, and the use of intermediaries to access the digital world.

[37] Supra note 87.
[38] Supra note 87.

An autonomous privacy framework based on user rights will not likely protect individuals who realistically cannot and will not navigate notices and consents, complaints, and processors. For the law to work in India, it cannot just work for the autonomous smartphone user, but also for those whose digital engagement is circumstantially and constrained mediated.

XIII. Commercial Interests, Governance, and National Security

The chapter illustrates the complexity of finding the right balance between privacy and commercial efficiency and the roles of governance and national security. The DPDP Act claims to try to achieve a balance of sorts. The reiteration of the right of individuals to protect their data and the right of the state to process data for the purposes of compliance in the long title of the Act demonstrates this. The issue is not that balance is sought. The issue is the type of balance in question, and who gets to set the parameters and scope of the balance. In the DPDP, the state and market participants seem to have more room to operate within these flexible pathways, while individuals have fewer, and more limited rights.

The law commercialises state interests through its comparatively liberal approach to transfers, exemptions for start-ups, flexible legitimate purposes, and light touch compliance. The interests of governance are located in section 7 and section 17, the state-processing rules, and the executive's significant control over the shaping of the implementation. The interests of national security are located in the exemption chapters and the rules-related access to information and retention of data during the rule.

Criticism from IFF after the 2025 Rules illustrates that Rule 8(3) states that fiduciaries must retain, if required by the State or its instrumentalities, personal the retention period is for at least one year after the purpose is achieved to include a longer period required by law. Such a rule may be understandable from a law-enforcement or security perspective, it nonetheless raises retention questions regarding the storage of logs that involve sensitive processing.[39]

There is a bigger problem at stake. Privacy law in India is being formulated in conjunction with a sweeping digital governance and data-based management of processes. In this context, the State is not an external referee between citizens and corporations. It is one of the largest data processors and one of the main profiteers of data-intensive systems. This shifts the imperative

[39] Jackson, K. (2024). Public and Private Fiduciaries: Representation in States, Corporations, Trusts and Agents. Ohio St. Bus. LJ, 19, 67.

for robust legislation to the extreme. When the system that promotes digitalisation also draws borders for itself and governs the theatre of the regulator, the equilibrium between privacy and governance is structurally compromised.

XIV. Civil Society, Policy Critique, and Emerging Consensus

This text is a bit rough so let's improve it. The majority of critics have raised relatively similar issues as civil society and policy criticism have highlighted. The Internet Freedom Foundation has criticisms including research exemptions, state-linked data retention, and the burdens of compliance/exemption design. The Centre for Internet and Society has raised concerns about the rules' consistency with the Act and questions regarding the governance of transfers. Numerous policy and scholarly commentaries have noted that while India's framework is a good start, it is still far too executive-driven and lacks the rights that more preferable models possess. Even some analyses that are supportive of the framework recognise that the Board, the application of rules, and whether the actions taken are more limiting than what exists within the law's discretionary boundaries will determine the overall success of the system.

This criticism is noteworthy because it shows that the primary issues with the DPDP Act are derived from the structure of the law and not stemming from ideological opponents of data governance or scholarly adversaries. The recurring issues highlighted in these criticisms are the same and are problematic in the law's structure. Problems include repeat issues such as unaccountable executive discretion, unaccounted rights, poorly defined limitations of state access, underdefined independence of the regulators, and uncertainty. Recurring criticism of these issues demonstrates that the problems with the law are structural, not solely technical.[40]

XV. Theoretical Assessment: Rights-Based or Compliance-Based?

The DPDP Act is a unique combination of both a rights-based legal privacy framework and a compliance-based administrative code. To say the DPDP Act ignores rights would be incorrect. The DPDP Act is concerned with compliance with the individual interest of the individual concerned with the protection of personal data. However, the machinery of the Directives, Operative, and Administrative Acts of Process is likely to be more concerned with the management of lawful processing than empowering a right of contestation. The DPDP Act's strength lies in the construction of detailed administrative regulations. The Directives,

[40] Supra note 92.

Operative, and Administrative Acts of Process set out detailed regulations for notice, consent, breach, reporting, officer appointments, auditor responsibilities, process, penalties, and breach reporting. The DPDP Act is weaker when it comes to regulation and a redistribution of power. State exemptions, structural gaps, algorithmic opacity, user objection, regulator independence, transparency, and other gaps remain in the Act. The implications of this are of even greater constitutional significance. Puttaswamy did not view privacy as a set of administrative entitlements. Puttaswamy viewed privacy as a condition of dignity, liberty, and personhood. Therefore, a genuinely post-Puttaswamy statute would do far more than merely regularise processing. The statute would centre the individual in the information order. The DPDP Act is headed in that direction and is likely to get there. It is not always about the constitutionalisation of privacy in words; it is about the structural and institutional depth of the Act.

CONCLUSION

The initial significant discovery in this article is that Indian data protection legislation is inextricably linked with constitutional privacy jurisprudence. The tale of the law begins with the initial, excessive judicial reluctance to accept the existence of privacy as a constitutional right, as seen in M.P. Sharma v. Satish Chandra and the majority opinion in Kharak Singh v. State of Uttar Pradesh. However, with the passage of time, the Supreme Court began to adopt a richer understanding of personhood and liberty. The cases of Gobind, R. Rajagopal, and PUCL, brought incremental changes to the legal protection of autonomy, reputation, domicile, communication, and confidentiality. The development was crowned by the Puttaswamy case, the nine-judge bench case that recognised the right to privacy as a fundamental right that is anchored in the provisions of Articles 14, 19, and 21 and also an integral part of the Right to Informational Privacy within the scope of the constitutional right to liberty and dignity. This constitutional perspective is significant because the DPDP Act is not a mere policy reaction to digitalisation; it is a legislative reaction to a constitutional imperative. With the recognition of Informational Privacy as part of the dignity, autonomy, and freedom of individuals, the State could not continue to use a patchwork of approaches like section 43A of the Information Technology Act and the SPDI Rules, 2011 as a reasonable alternative to a comprehensive regulatory regime.

The DPDP Act arose not just because data had an economic value, but also because there was constitutional law soliciting a framework for the regulation of the power of information in a

manner that recognises the associated rights. The second major finding is that the DPDP Act has, in fact, established a baseline data protection framework, albeit in a minimalist, executive-centric way. The Act acknowledges the individual's right to self-authoring through personal data protection, establishes a notice-and-consent framework, imposes duties on data fiduciaries, rights on data principals, breach notifications, significant penalties, and establishes the Data Protection Board of India. These are significant developments, and a far cry from the previous legal vacuum that existed. However, the Act is far from representing a mature rights-based privacy code. It lacks several rights, provides little detail in stronger systems, leaves a great deal of information to be controlled by rules and notifications, and is permissive of non-consensual processing and state-facing exemptions.

The third major finding identifies the central constitutional defect of the Act to be the tension between its rights rhetoric, and its discretionary framework. The law recognises the importance of privacy, but also gives the executive branch a great deal of power in the areas of initiation, rulemaking, exceptions, cross-border transfer limitations, the classification of major data fiduciaries, and the structural design of the Board. This power is, in a way, a non-decision on governance. It determines the elasticity of privacy as a policy concern for the State, as opposed to something more poignant which is a legal right that governs the State. The fourth key finding is that litigation concerning the Act is beginning to raise constitutional questions. In February 2026, the Supreme Court, while refusing to stay the law, passed on the pleas regarding amendments to the Right to Information Act and the DPDP framework to a larger bench. This indicates that the Indian data protection law is in the stage of constitutional contestation as much as it is in the stage of implementation. Both adjudication and regulation will define the law's future.

I. Does the DPDP Act Adequately Operationalize Informational Privacy?

An important question in this article is how fully the DPDP Act constitutes the right to privacy regarding personal data. While the answer is partially positive, the Act only reflects the right to privacy in a constitutionally prominent and legally necessary manner. However, it has yet to capture the full normative depth of the right to privacy articulated in Puttaswamy.

There are, however, instances where the DPDP Act does so positively. The Act shows, to some degree, recognition of the fact that individuals have a legal interest in the privacy of their personal data. Subsequently, the Act posits the idea of roles such as data principal, data

fiduciary, consent manager, and significant data fiduciary. It additionally proposes that consent be free, specific, informed, and folded into the clause by notice, as well as being unconditional and unambiguous. It proposes the requirement of reasonable safeguards to preserve security, the right to be notified of any breaches, as well as the right to access, correct, and in certain instances, the right to erase, as well as to redress grievances and to nominate. The Act, in some respects, also provides greater obligations in favour of significant data fiduciaries, as well as providing special consideration for children and protecting them against tracking, behavioural monitoring, and targeting advertisements. Certainly, all of these additions transcend mere accomplishments. They transform privacy in the Puttaswamy case from mere a constitutional abstraction to a system of legally defined and legislatively actionable privatized grievances and remedies. However, four important constitutional elements are still missing. First, the breadth of the rights catalogue is limited.

It neither grants a general right to object to processing nor a general right to data portability, nor a general right to impose restrictions on processing, nor an 'express' right not to be subject to significant automated decision-making. In the current data economy, with its incessant and continuous operations of algorithmic systems that analyse and act on personal characteristics, these omissions are significant. While some may view informational privacy as solely the access and correction, it encompasses much more, and includes, the right to resist, contest and reform the persistent operation of data-driven decision-making systems.

The second point relates to the undue burden that the Act places on the concept of consent. It is true that, in regard to the concept of consent, a number of issues have been identified, including consent fatigue, unequal bargaining power, digital vulnerability, language and culture, the design of the platforms, and so forth. Although the consent language is robust from a legal standpoint, the context in which that consent is sought penalises the prospect of exercising a meaningful choice. This is further complicated by the fact that broad "certain legitimate purposes" categories allow significant processing to occur without consent. Hence, it may be that consent is functionally and operationally central, but structurally it is not central.

Then, the design of exemptions in the statute is, in a way, that it is difficult to deal with the proportionality test as outlined in Puttaswamy. A privacy law may allow for a limited number of deviations for national security, public order and public health emergencies, legal compliance and the administration of the state. However, such departures must be narrowly

defined and accompanied by meaningful safeguards. The Act's broad exemption powers, particularly regarding the State and state instrumentalities, make it difficult to argue that the framework adequately incorporates the privacy implicating power of public governance.

The fourth factor is that institutional design inhibits enforcement. There is a Data Protection Board, but existing structural independence is not stronger than in less developed systems. Appointment, terms of employment, composition, staffing, and most procedural frameworks are under considerable Central Government control. That is particularly troubling in an area in which the State is one of the largest and most significant personal data processors. A privacy framework that applies to the public and private spheres must have a regulator that is not only operationally functional but independent in appearance.

For these reasons, the article concludes that the DPDP Act is not able to fully implement, in a constitutional sense, the right to informational privacy. It does create a statutory scheme for data governance, but it does not fully protect privacy, as a fundamental right, against the disproportionate power of the state and the market. It is an initial step, not a definitive constitutional arrangement.