INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CONSENT UNDER SIEGE: CORPORATE DATA POWER, CONSUMER VULNERABILITY, AND THE INCOMPLETE PROMISE OF INDIA'S DIGITAL PRIVACY

AUTHORED BY - HARINI KARTHIKEYAN & POOJASHREE R
4th Year, B.A. LL.B. (Hons.), SASTRA Deemed University

ABSTRACT

The Digital Personal Data Protection Act, 2023 is India's first attempt to define data privacy as a consumer right under law, rather than as a contractual concession. However, the framework is built around a fundamental contradiction — it empowers individual data principals while simultaneously concentrating enormous power with the executive through wide state exemptions, with critical aspects of the privacy right left to subordinate legislation. This article assesses how the Act positions data privacy within the digital Indian economy; it analyses the consent regime, consumers' rights, the Data Protection Board, and cross-border data transfers. While recognising the structural strengths of the Indian framework in comparison with the European Union's General Data Protection Regulation and Brazil's Lei Geral de Proteção de Dados, the article contends that the framework is marred by three key problems: an over-reliance on deemed consent, which undermines the very notion of consumer agency; a Data Protection Board that is insufficiently independent to ensure genuine accountability; and a state exemption clause that is excessively broad. Finally, it offers recommendations on how the law should be strengthened in order to achieve what it sets out to do: protect the right of individuals to privacy over their data as consumers.

Keywords: Digital Personal Data Protection Act, 2023; Data Privacy; Consumer Rights; Consent; Data Protection Board.

I. Introduction: The Datafied Consumer and the Question of Rights

Every time an Indian consumer logs onto a food delivery app, applies for an online loan, or signs up on a government scheme registration portal, they surrender some quantity of personal data whose worth, and whose subsequent life, they cannot see, challenge, or recover. In the contemporary digital economy, this asymmetry is constitutive of it; at the level of the corporation and state entities, vast quantities of individual personal data are harvested, analysed, and commercially exploited, while

ISSN: 2582-6433

at the level of the individual, there is either no transparency or no meaningful locus of control over data processing. This arrangement governed India for close to ten years through the Information Technology Act, 2000 and its 2011 Rules — instruments framed in a different technological milieu and fundamentally unsuited for the algorithmic logic of platform capitalism.[1]

It was against this backdrop of regulatory absence and constitutional necessity that the Digital Personal Data Protection Act, 2023 was enacted.[2] The Act's roots trace to the landmark judgment in *Justice K.S. Puttaswamy v. Union of India*, [3] whereby a nine-judge bench of the Supreme Court unanimously declared privacy to be a fundamental right guaranteed by Article 21 of the Constitution. The judgment affirmed an affirmative constitutional duty on the legislature to provide a legal framework to translate the right to informational self-determination from judicial abstraction to legal certainty. The DPDPA is the legislature's reply.

The importance of this moment cannot be overstated. India has more than 750 million internet users, the largest digital identity programme in the world in Aadhaar, and a booming platform economy that has attracted both significant global capital and unprecedented global scrutiny. The question of whether the DPDPA truly secures data privacy as a consumer right — or merely offers its semblance through carve-outs, delegated discretion, and institutional frailties — thus extends far beyond the theoretical and is of critical significance for the democratic dimension of India's digital future.

This article presents the DPDPA under five heads: Part II considers the doctrinal and constitutional basis of consumer data privacy in India; Part III delves into the consent regime and rights framework under the Act; Part IV analyses the institutional design of the Data Protection Board and its efficacy as a remedy; Part V addresses cross-border data flows and the geopolitical implications of the DPDPA; and Part VI reviews the DPDPA critically in the context of international practices and concludes with recommendations.

II. Constitutional Foundations: From Judicial Mandate to Statutory Right

A. The Privacy Judgment and Its Structural Dimensions

The intellectual architecture of Indian data protection law begins not in Parliament, but in the hallowed chambers of the Supreme Court. In *Puttaswamy* (2017),[4] the nine judges arrived at unanimous conclusions — privacy is constitutionally protected — though their reasoning unfolded in six separate judgments, which nonetheless coalesced on a few propositions. Privacy is not a singular, indivisible

[1]The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).
[2]Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDPA].
[3]Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, ¶ 1 (India) (nine-judge bench unanimously declaring privacy a fundamental right under Article 21 of the Constitution of India).
[4]Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

ISSN: 2582-6433

right, but a collection of interests including bodily integrity, decisional autonomy, and, importantly, informational privacy — the right of an individual to control the narrative of one's own data.[5]

Justice D.Y. Chandrachud's judgment, which is perhaps the most analytically robust amongst the six opinions, framed informational privacy in the concept of contextual integrity — which essentially states that personal data disclosed in one social context cannot justifiably be used in a different context without the notice and consent of the data subject.[6] The implication of such a framework for regulation is direct; it requires data to not merely be kept safe from breaches, but that collection, purpose, retention, and data transfer should also be governed by norms that respect the contextual terms in which data was originally disclosed. A regime that collects personal data for the purpose of state subsidy cannot re-purpose such data for profiling without infringing on the fundamental right. The *Puttaswamy* judgment has thus set the constitutional threshold for any data protection statute; to pass constitutional muster, it will be judged against a proportionality test. A restriction on the right to privacy can only be made by law if it has a legitimate objective, is necessary for the said objective, and is proportionate to it.[7]

B. The Pre-Legislative Journey: The Srikrishna Committee and the Data Subject

A more elaborate conceptualisation of data privacy is offered by the Srikrishna Committee Report (published in 2018, prior to five years of legislative gestation leading to the DPDPA), which provides us with the notion of the individual possessing a proprietary right — akin to an ownership right in terms of common law property — over personal data; though it is not a right to actual ownership but a right to stewardship or control over their data, regardless of whose physical possession it may lie in.[8] It takes the debate out of the contractual domain where the consumer is considered to have consented because he entered into a contract where sharing of data was one of the terms, and places the consumer in a position of controlled agency. While the final Act deviates from some of the more robust provisions drafted in the Committee Report — such as requirements for data localisation and stricter limitations on grounds for processing — the individual-centric rights framework, where the consumer is seen not merely as a data subject but as a data principal with enforceable rights, has been successfully legislated into the Act.

III. The Architecture of Rights and the Paradox of Consent

[5]Id. ¶¶ 144–169 (Chandrachud, J., concurring) (elaborating the tripartite structure of the right to privacy as encompassing bodily integrity, decisional autonomy, and informational privacy).
[6]Id. ¶ 180 (Chandrachud, J., concurring). See also Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life 127–157 (Stanford Univ. Press 2010) (developing the theory of contextual integrity as the normative basis for evaluating information flows).
[7]Puttaswamy, (2017) 10 SCC 1, ¶¶ 310–315 (Chandrachud, J., concurring) (articulating the proportionality test as: (i) legitimate aim; (ii) rational nexus; (iii) necessity; and (iv) proportionality stricto sensu).
[8]Justice B.N. Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians — Report of the Committee of Experts on Data Protection 18–22 (Ministry of Electronics and Information Technology, 2018) [hereinafter Srikrishna Committee Report].

ISSN: 2582-6433

A. Consent as the Foundation of Lawfulness

At the very heart of the DPDPA's framework for protecting consumers is the concept of consent. Under Section 4, personal data may be processed only for lawful purposes, with lawful processing being predicated on either free, specific, and informed consent given by the data principal, or on the statutorily presumed consent deemed to be given on the grounds enumerated in Section 12.[9] Consent must be obtained through a clear notice in plain language containing the categories of personal data to be collected and the specific purposes for which such data will be used.[10]

In theory, the consent model has genuine transformative potential. It changes the role of the data principal from being an inert subject of data to an active rights-holder, empowered to consent, condition, and restrict consent to data processing. Crucially, Section 16 stipulates the right to withdraw consent at any time, recognising that the consumer's relationship with their data is ongoing and that consent once given is not an irrevocable licence.[11]

But the framework operates within structural realities that undermine its promise. A digital economy in India where essential services — from government portals to predominant platform intermediaries and core payment infrastructure — impose practically unalterable terms and conditions systematically overrides any meaningful possibility of a genuinely free consent model. The GDPR addresses this by prohibiting conditioning service delivery on data processing beyond what is strictly necessary for the provision of the service.[12] The DPDPA, lacking this prohibition, forces consumers into a framework where giving consent is practically mandatory if they wish to receive the service. Consent will, more often than not, become coerced rather than freely given — a ritualistic check-box that the literal provisions of the law require but that undermines the normative goal of the Act.[13]

B. Deemed Consent: The Structural Flaw

Section 12, concerning deemed consent, is perhaps the most critical structural fault in the entire consumer protection regime envisioned under the Act. Deemed consent permits data processing without express consent where processing is required to perform a function of the State, comply with a court or tribunal order, process employee data, respond to a medical emergency, or conduct public-interest

[9]DPDPA § 4.
[10]DPDPA § 5 (prescribing the form and content of notice to be provided to data principals prior to or at the time of collection of personal data).
[11]DPDPA § 16(1) (providing that a data principal may withdraw consent at any time, subject to the consequences of such withdrawal).
[12]Commission Regulation 2016/679, art. 7(4), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR] ("When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract... is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.").
[13]Cf. Norwegian Consumer Council, Deceived by Design: How Technology Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy 5–9 (2018) (documenting the prevalence of dark patterns and coercive consent mechanisms in digital platforms).

ISSN: 2582-6433

research.[14] Each of these scenarios has some logical basis. However, when viewed in the context of the increasing datafication of a state whose services range from welfare delivery to tax administration, law enforcement, and identity verification, the scope of deemed consent becomes alarming.

Shoshana Zuboff states that the defining characteristic of the digital economy is not its misuse but its "normalised extraction," where data surrender is treated not as a voluntary exchange but as a prerequisite to social participation.[15] Deemed consent essentially builds such logic into statute, legitimising state data processing wherever the State perceives itself performing a "function." The *Puttaswamy* requirement of strict proportionality means that any intrusion on privacy must be narrowly tailored and involve the minimum amount of data processing necessary. The grounds of deemed consent as they exist in Section 12 do not fulfil this requirement — they define categories of processing without any stipulation on proportionality, necessity, or the absence of alternative, less intrusive modes of processing. This gap between the Act's ambiguity and constitutional requirement opens a loophole for both corporations claiming state-like functions and for the State itself to proceed with data processing on the basis of broadly stated reasons.

C. Data Principal's Rights: Promise and Gap

The DPDPA's rights framework, as provided under Sections 16 and 17, confers numerous rights on the data principal — a significant improvement over the existing framework under the IT Act. These rights include a right to a summary of personal data being processed, a right to correction and erasure, a right to grievance redressal, a right to nominate a representative in case of death or incapacitation, and the right to approach the Data Protection Board.[16] When compared with international counterparts, the framework provides contextually sensitive alternatives to the universal approach. For instance, the right to nominate a representative is significant; in an Indian context where digital accounts have significance beyond the immediate user even after their demise, it serves to fill a lacuna that many legal regimes, including the GDPR, have not systematically addressed.[17]

Nevertheless, the Act possesses several crucial lacunae. Most significantly, it lacks a data portability right equivalent to Article 20 of the GDPR — the right to receive personal data in a machine-readable format and transfer it to another data fiduciary. Data portability is not a mere optional extra in an Indian economy where platform lock-in and data moats built by dominant players significantly

[14]DPDPA § 12 (enumerating the grounds of deemed consent, including processing necessary to perform a function of the State, comply with a judicial order, process employment data, respond to medical emergencies, and conduct public-interest research).
[15]Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power 11–13 (PublicAffairs 2019).
[16]DPDPA §§ 16–17.
[17]GDPR arts. 17–20 (providing rights of erasure, restriction of processing, and data portability, but containing no specific provision for nominee rights upon the death or incapacitation of the data subject). See also Srikrishna Committee Report, supra note 8, at 36 (recommending inclusion of a nominee right in light of Indian social realities).

ISSN: 2582-6433

distort competition and consumer choice; it is a vital tool for empowerment. Its exclusion reveals the legislative priority afforded to vested corporate interests over consumer choice and agency. Further, the Act fails to explicitly grant data principals a right to object to processing or protection from solely automated decision-making — rights that form the very backbone of the GDPR and are particularly important given the reliance of crucial processes such as credit scoring, insurance underwriting, and recruitment on opaque algorithms.

IV. Institutional Design: The Data Protection Board and the Problem of Independence

A. The Design of the Board and the Constraints of Its Structure

The enforceability of a rights framework is only as strong as the institution mandated to give effect to its principles. The DPDPA establishes the Data Protection Board of India, pursuant to Sections 27 to 30, as the primary adjudicatory body to investigate complaints, adjudicate breaches of data fiduciary obligations, and impose penalties.[18] The Board has powers to hear complaints of data principals, investigate contraventions, issue directions, and impose monetary penalties of up to ₹250 crore.

The structure in which the Data Protection Board is proposed to be set up raises basic questions about its autonomy from the Executive. Appointments to the Board rest with the Central Government, on the recommendations of a Selection Committee constituted by it.[19] There are no provisions that guarantee a fixed tenure for members of the Board, nor specifications regarding conditions of removal that would insulate members from politically motivated decision-making. This stands in contrast with the clear stipulation in the GDPR that data protection supervisory authorities must function "in full independence" from governmental influence.[20]

Institutional independence is critical to the meaningful enforcement of data protection rules. The most impactful enforcement actions under any regime are against dominant technology providers or state entities and public-private collaborations. An institution structurally dependent on the Executive will, predictably, refrain from such action. The experience of the European Union is illuminating: the Irish Data Protection Commission faced sustained criticism for its long inaction against Silicon Valley companies precisely owing to structural disincentives against vigorous enforcement. A similar systemic problem confronts India's Data Protection Board.

A much better institutional model has already been developed in India: the Securities and

[18]DPDPA §§ 27–30 (establishing the Data Protection Board of India, prescribing its composition, powers, and adjudicatory procedure).
[19]DPDPA § 27(2) (providing that the Chairperson and members of the Board shall be appointed by the Central Government on the recommendation of a Selection Committee constituted by it).
[20]GDPR art. 52(1) ("Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.").

ISSN: 2582-6433

Exchange Board of India[21] and the Telecom Regulatory Authority of India[22] have legislated guarantees of independence for their regulators, with statutory provisions on appointment, tenure, and budgetary autonomy. The DPDPA should have built upon India's established regulatory model, rather than establishing a body that operates closer to a government-appointed tribunal than an independent regulatory authority.

B. Penalties, Deterrence, and the Missing Accountability Logic

The penalty regime established by the Act may not serve as a sufficient deterrent against the biggest data fiduciaries. Though ₹250 crore is significant for the domestic market, it amounts to a small fraction of the global platforms' annual revenue generated within India. The European Union's penalty system — up to 4% of global annual turnover — was consciously framed to ensure that penalties exceed a mere cost of doing business for large players. The Act's fixed cap creates a rational calculus for big-tech companies: if anticipated compliance costs exceed expected penalty-weighted values, data fiduciaries may choose non-compliance.

The Act also excludes a private right of action for data principals against data fiduciaries for violation of the Act. All complaints are channelled through the Data Protection Board, resulting in a concentration of power at one point and the exclusion of individual legal remedy through individual claims or class actions. California's CCPA, for example, provides a private right of action against data fiduciaries in cases of data breach.[23] India's omission of such a right further augments the concentrated powers at an already structurally weakened institution.

V. Cross-Border Data Flows, State Exemptions, and the Problem of Sovereignty

A. Transfer Mechanisms: Notification-Based Whitelisting

The mechanism for cross-border data transfers under Section 33 of the DPDPA is government-led whitelisting: personal data may only be transferred to such countries as may be notified by the Central Government.[24] The model grants the national executive broad authority in determining both the

[21]Securities and Exchange Board of India Act, 1992, No. 15, Acts of Parliament, 1992, § 16 (India) (providing statutory tenure and conditions of removal for SEBI board members, insulating them from executive interference).
[22]Telecom Regulatory Authority of India Act, 1997, No. 24, Acts of Parliament, 1997, §§ 5–6 (India) (establishing tenure protections and independent adjudicatory mechanisms for TRAI).
[23]California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.150 (West 2023) (creating a private right of action for consumers whose personal information is subject to unauthorised access due to a business's failure to implement reasonable security procedures and practices).
[24]DPDPA § 33 (empowering the Central Government to notify countries or territories to which personal data may be transferred, subject to such terms and conditions as may be prescribed).

ISSN: 2582-6433

criteria and the process by which designated transfer destinations will be vetted. This departs substantially from the mechanism set forth in the GDPR, which is rooted in adequacy decisions of the European Commission and in supplementary instruments such as standard contractual clauses and binding corporate rules that operate without member state executive discretion.[25]

While the whitelisting approach has obvious geopolitical attractions — allowing India to leverage its decisions on permitted data transfers for reciprocal market access and data governance arrangements — it creates significant uncertainty for both consumers and businesses alike. In the absence of clear criteria determining which countries receive designation for transfer purposes, destinations may be approved or denied on considerations unrelated to actual data protection standards in the recipient country. The Schrems I judgment from the Court of Justice of the European Union famously found that data transfer arrangements based on governmental guarantees rather than independently verifiable legal standards are structurally fragile.[26] India's framework offers less transparency of the criteria for whitelisting, making such structural fragility highly probable — akin to the position under China's Personal Information Protection Law, which requires a security assessment before cross-border transfers but has also been used to facilitate surveillance purposes rather than consumer protection.[27] Concentrating cross-border transfer authority in the hands of the executive without parliamentary oversight of the whitelisting criteria risks the same fate for India's data protection law.

B. The State Exemptions: Privacy's Constitutional Nemesis

The most serious constitutional issue — and by far the most dangerous provision within the DPDPA — is the state exemption under Section 18. The government may exempt any agency from all or any part of the provisions of this Act if it determines it is necessary in the interests of the sovereignty, integrity, and security of India, public order, or the maintenance of friendly relations with foreign states.[28]

The criteria used to determine the applicability of such exemptions are so expansive that the provision appears practically limitless. The broad categories — sovereignty, security, public order —

[25]GDPR arts. 45–46 (establishing adequacy decisions and supplementary transfer mechanisms, including standard contractual clauses and binding corporate rules, as the permissible bases for international data transfers).
[26]Maximillian Schrems v. Data Protection Commissioner (Schrems I), Case C-362/14, ECLI:EU:C:2015:650 (Court of Justice of the European Union, Oct. 6, 2015) (invalidating the EU-US Safe Harbour arrangement on grounds that governmental self-certification without independent legal standards did not provide adequate protection).
[27]Personal Information Protection Law of the People's Republic of China (promulgated by the Standing Committee of the National People's Congress, Aug. 20, 2021, effective Nov. 1, 2021), art. 38 (requiring security assessment prior to cross-border transfer of personal information). See also Paul Triolo et al., The Geopolitics of China's Data Governance Framework, Eurasia Group Report 12–16 (2022) (arguing that China's data transfer regime prioritises state surveillance over consumer protection).
[28]DPDPA § 18 (authorising the Central Government to exempt any instrumentality of the State from the application of all or any provisions of the Act in the interests of the sovereignty and integrity of India, security of the State, friendly relations with foreign states, or public order).

ISSN: 2582-6433

are precisely the vague grounds the Supreme Court warned against in *Puttaswamy*, requiring strict proportionality review to constitute valid restrictions on fundamental rights.[29] By granting the state a full exemption not just from data protection duties but from any notice, correction, or erasure requirements necessary for data principals to assert their constitutional privacy rights, this exemption completely negates the law's ability to regulate the state.

The amendment already inserted into Section 8(1)(j) of the Right to Information Act, 2005, limiting access to personal information when public interest dictates otherwise,[30][31] read together with Section 18 of the DPDPA, means that the state's data practices will continually be removed from any possibility of challenge or regulation under both data protection law and transparency law. The individual consumer will, in fact, face the greatest exposure to data exploitation precisely where the data fiduciary is the state rather than a private company.

VI. Comparative Assessment and Proposals for Reform

A. India in the Global Data Governance Landscape

A survey of data protection regimes around the world reveals India to be something of an anomaly. It offers more than the previous sectoral, consent-light regime, and its rights framework is stronger than some developing-economy privacy legislation. But by the standards of the global gold standard — the GDPR — it is lacking in three critical respects: consent protection; institutional independence of the enforcement authority; and state accountability.[32][33]

Brazil's Lei Geral de Proteção de Dados Pessoais (LGPD) is a pertinent case in point. In a similarly complex federal democracy with extensive platform economy interest groups and a powerful surveillance state, the LGPD created an independent data protection authority — the Autoridade Nacional de Proteção de Dados — with constitutional status and structural insulation from executive interference.[34] By contrast, the DPDPA's Board is situated within the executive, with appointments

[29]Puttaswamy, (2017) 10 SCC 1, ¶¶ 310–315 (requiring that restrictions on the right to privacy satisfy a four-part proportionality test, including the requirement that the measure be the least restrictive means of achieving the legitimate aim).

[30]Right to Information Act, 2005, No. 22, Acts of Parliament, 2005, § 8(1)(j) (India) (exempting from disclosure personal information whose revelation has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual).

[31]The Digital Personal Data Protection Act, 2023 amends § 8(1)(j) of the Right to Information Act, 2005 to expand the personal information exemption, thereby narrowing the scope of transparency available to citizens regarding state data practices. DPDPA § 44(3).

[32]Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives 14–22 (Oxford Univ. Press 2014) (surveying comparative data protection regimes in Asia and assessing their divergence from the GDPR standard).

[33]Usha Ramanathan, A Unique Identity Bill, 46 Econ. & Pol. Wkly. 10, 10–14 (2010) (analysing structural tensions between the Indian state's data collection imperatives and individual privacy rights in the pre-DPDPA framework).

[34]Lei Geral de Proteção de Dados Pessoais [LGPD], Lei No. 13.709, de 14 de agosto de 2018 (Braz.), arts. 55-A to 55-L (establishing the Autoridade Nacional de Proteção de Dados with constitutional recognition, structural independence, and its own budgetary allocation).

ISSN: 2582-6433

ultimately determined by government and no structural guarantee of budgetary autonomy — a clear institutional weakness.

The California Consumer Privacy Act and California Privacy Rights Act (CCPA/CPRA) demonstrate how a robust consumer-centric regime may be developed without a sweeping GDPR-style overhaul.[35] The opt-out notice rights, opt-out of data sale rights, and private right of action provided in the CCPA are absent from the DPDPA and represent tractable reforms that do not require restructuring the entire Act.

B. Proposals for a More Protective Framework

The proposals below are offered with a view to strengthening the consumer-facing aspects of the DPDPA, without fundamentally rewriting the entire structure of the Act.

First, the concept of deemed consent under Section 12 should be made more granular through the insertion of a proportionality test: processing based on deemed consent is permissible only when necessary for the declared purpose and only to the extent that no less privacy-invasive means are reasonably available. This integrates constitutional doctrine directly into statutory law and helps narrow the gap between *Puttaswamy's* jurisprudence and legislative action.

Second, there should be a fundamental reform of the Data Protection Board to create institutional independence. At a minimum, this implies statutory tenure for members, requiring removal only for cause as defined by the statute with judicial review by the Supreme Court, independent budgetary control not subject to executive discretion, and the inclusion of civil society members and technical experts in the selection process. The Competition Commission of India offers an example of an institution with structural independence, even if practical contestation persists.

Third, the state exemption under Section 18 must be placed under an explicit proportionality test and parliamentary oversight. Any notification exempting a state agency must articulate the specific purpose, category of data or obligation to be exempted, and duration of the exemption. Such notifications must be tabled before Parliament and require a negative parliamentary resolution to enter into force. This does not eviscerate the state's ability to manage data for security interests, but places it under the constitutional scrutiny it requires.

Fourth, through rule-making power under Section 40 or direct amendment, rights of data portability and objection to automated decision-making should be included. These are not niceties in a data economy; they are practical rights enabling user control.[36]

[35]California Consumer Privacy Act of 2018 (CCPA), Cal. Civ. Code §§ 1798.100–1798.199 (West 2023); California Privacy Rights Act of 2020 (CPRA), Cal. Civ. Code § 1798.185 (West 2023) (amending and strengthening the CCPA by establishing the California Privacy Protection Agency as an independent enforcement authority and creating opt-out rights from the sale and sharing of personal information).

[36]GDPR arts. 20–22 (providing data subjects with rights of portability, objection to processing, and protection from solely automated decision-making including profiling). See also Srikrishna Committee Report, supra note 8, at 40–43 (recommending inclusion of a data portability right in the Indian data protection framework).

ISSN: 2582-6433

Fifth and finally, a qualified private right of action for data principals in cases of personal data breach should be established. This diffuses enforcement responsibility beyond a single government agency and across the consumer base, creating a more resilient framework for accountability.

VII. Conclusion

The Digital Personal Data Protection Act, 2023 represents a significant legislative step: for the first time, India possesses an enacted law that establishes data privacy as a consumer right, frames the duties and responsibilities of Data Fiduciaries, and sets up an adjudicatory forum to implement it. The constitutional basis of *Puttaswamy* not only made its way into the preamble of the Act[37] but was effectively embodied in its substantive provisions as well, and the individual's persona as Data Principal bestowed with enforceable entitlements is a novel idea that moves beyond the transactional nature of the old Act.[38]

However, a right enshrined in law and a right which can be exercised are different concepts. Vulnerabilities rooted in the consent mechanism of the Act, the lack of impartiality of the Board, the overbreadth of the state exemption, and the non-inclusion of portability rights and a private right of action together construct a scheme that allows consumers to use the language of rights without altering the environment in which those rights are most likely to be denied. The inclusion of the state as a Data Fiduciary — and, in India's digital ecosystem, its most powerful one — while simultaneously exempting it from rules that apply to other data fiduciaries, and situating the data protection regulator within the executive apparatus, means that the enacted regime is neither neutral nor equitable.

The proposals offered in this article are not deviations from the enacted law; rather, they seek to complement it. They ask for data protection provisions that are commensurate with the fundamental right they are intended to put into practice. *Puttaswamy* defined the right to informational self-determination as a fundamental human right — not a regulatory preference to be abandoned when inconvenient. India's data protection regime will only live up to its constitutional promise when the design of its institutions, its framework of exemptions, and its mechanisms for enforcement match the constitutional gravitas of the right it is intended to defend.

[37]DPDPA, Preamble (affirming the right to privacy as a fundamental right and the need to protect the digital personal data of individuals while recognising the legitimate uses for which data may be processed).
[38]Id. §§ 16–17 (conferring enumerated rights on data principals, including rights of access, correction, erasure, grievance redressal, and nomination).