PANJAB UNIVERSITY LAW REVIEW
ISSN: 0971-5541, Volume 64, Part 1, pp. 187-199

DATA PROTECTION AND CONSUMER RIGHTS IN THE DIGITAL AGE: TOWARDS A CONSUMER-CENTRIC LEGAL FRAMEWORK IN INDIA

Meenakshi[*]
Dr. Rita Thakur[**]

ABSTRACT

In India's rapidly evolving digital landscape, personal data has become both a critical economic asset and a source of consumer vulnerability. With nearly a billion internet users and growing dependence on digital platforms, consumers routinely share sensitive information, often without clear consent or a meaningful understanding of how that information will be used. This paper examines the relationship between data protection and consumer rights in India, asking whether current law adequately safeguards individuals in the digital marketplace. The Digital Personal Data Protection Act, 2023, together with the Draft Digital Personal Data Protection Rules, 2025, marks a significant step toward structured data governance, yet substantial challenges remain, including weak enforcement capacity, limited public awareness, and persistent risks of data breach, algorithmic profiling and unfair terms of service. The paper situates India's framework against global benchmarks, the European Union's General Data Protection Regulation, the United Nations Guidelines for Consumer Protection, and the sectoral United States model, and draws on constitutional case law, statutory text and documented breach incidents to assess the adequacy of India's current regime. It concludes that India's data protection architecture, while a genuine advance over its fragmented predecessor, requires stronger institutional independence, clearer procedural rules and sustained public education before it can deliver the consumer-centric protection its text promises.

KEYWORDS: *Data Protection; Consumer Rights; Digital Privacy; DPDP Act 2023; Comparative Data Governance*

1. INTRODUCTION

India, with its vast population and dynamic digital ecosystem, sits at the forefront of the world's ongoing digital transformation. As commerce, banking, healthcare and entertainment have migrated online, personal data has become a form of currency: every transaction leaves behind a digital footprint, names, contact details, preferences, location, and increasingly sensitive financial or health information, that businesses collect to personalise services and improve user experience while simultaneously exposing consumers to data breach, identity theft, algorithmic profiling and unauthorised surveillance. India's total internet subscriber base grew from 251.59 million in March 2014 to 954.40 million in March 2024, and the country was home to 491 million social media user identities by January 2025, representing roughly 33.7 per cent of the total population.[1] The scale of this user base is matched by a correspondingly large exposure to risk, since consumers routinely share personal information without

[*] Research Scholar, Department of Laws, Panjab University, Chandigarh.
[**] Assistant Professor, University School of Law, Rayat Bahra University, Mohali

[1] Ministry of Communications, Azadi Ka Amrit Mahotsav: Universal Connectivity and Digital India Initiatives Reaching All Areas, Press Information Bureau (Aug. 2, 2024); Simon Kemp, Digital 2025: India, DataReportal (Feb. 25, 2025).

understanding the implications of doing so, a gap the country's evolving legal framework has only recently begun to close.

Data protection refers to the legal and technological frameworks governing the collection, processing, storage and sharing of personal data, and it plays a central role in ensuring that consumer rights are respected within the digital marketplace. For an extended period, India's approach to this problem remained fragmented and inadequate: privacy protection rested on the minimal provisions of the Information Technology Act, 2000, while a dedicated privacy statute remained in legislative limbo for the better part of a decade. The Right to Privacy, recognised as an intrinsic facet of the right to life and personal liberty under Article 21 of the Constitution, supplied the constitutional foundation on which reform would eventually be built, empowering individuals in principle to control the use and disclosure of their personal information even before statutory protection caught up with that constitutional promise.[2] The enactment of the Digital Personal Data Protection Act, 2023, India's first comprehensive digital privacy legislation, and the subsequent release of the Draft Digital Personal Data Protection Rules, 2025 for public consultation, mark the most significant response to this gap to date. This paper asks whether these instruments, individually and together, are adequate to protect Indian consumers in the digital space, whether the entities that collect and process consumer data are genuinely held accountable under them, and whether consumers themselves are positioned to understand and exercise the rights the law now affords them.

1.1 Objectives of the Study

This study aims to trace the evolution of data protection legislation in India, from the Personal Data Protection Bill, 2019 to the enactment of the Digital Personal Data Protection Act, 2023 and the Draft Rules of 2025; to examine the current legal framework governing digital personal data and assess its effectiveness in protecting consumer rights; to identify the principal challenges consumers face in safeguarding personal data within an increasingly surveillance-driven digital environment; to evaluate whether recent legal developments adequately balance the right to privacy against the legitimate interests of business and the State; and to offer practical suggestions for strengthening consumer data protection, public awareness, enforcement and institutional accountability under the existing regime.

This study adopts a doctrinal and analytical approach, relying primarily on secondary sources including statutes, case law, official reports, academic literature and credible reporting on documented data protection incidents, with particular reference to the Digital Personal Data Protection Act, 2023 and the Draft Rules of 2025. The research is qualitative, directed at identifying gaps in

---

[2] The Constitution of India, 1950, art. 21; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

the current legal structure and proposing improvements that are practical, consumer-oriented, and consistent with prevailing global privacy standards.

2. CONCEPTUAL FRAMEWORK: PERSONAL DATA, PRIVACY AND CONSUMER RIGHTS

Section 2(t) of the Digital Personal Data Protection Act, 2023 defines personal data broadly, as any information relating to an identifiable individual, encompassing names, addresses, IP details, biometric records and behavioural patterns gathered through digital activity.[3] Notably, the Act does not carve out a distinct, more stringently protected category of "sensitive personal data," financial detail, health record, sexual orientation or religious belief, of the kind explicitly recognised under the European Union's General Data Protection Regulation, an omission this paper returns to in Part 4. Data privacy in ordinary usage concerns the handling of what is often termed personally identifiable information, and the governing legal concept is informational privacy: the individual's right to control the collection, use and dissemination of data concerning them, a conception that moves beyond privacy as mere seclusion toward privacy as an expression of personal autonomy and dignity within a digitally mediated society.

As digital technology has matured, personal data has become a commodity in its own right, collected, traded, analysed and monetised by corporations frequently without the meaningful consent or awareness of the individuals to whom it pertains. This transformation has produced a structural imbalance between consumers and data controllers, in which consumers risk being reduced to data points within automated decision-making processes rather than treated as rights-bearing participants in the digital economy. Understanding the intersection between data protection and consumer rights accordingly requires a reconceptualisation of consumer protection itself: traditional consumer law addressed unfair trade practice and product defect, but the modern consumer additionally requires protection against unauthorised data harvesting, algorithmic profiling and surveillance-based advertising, harms that traditional consumer protection doctrine was never designed to reach. This paper treats personal data as simultaneously a legal category and a matter of lived consequence for the individual, connecting privacy, dignity, trust and fairness as the interpretive lens through which India's statutory response should be assessed.

The conceptual shift this framework requires is worth stating explicitly, since it underlies much of the analysis in the parts that follow. Classical consumer protection law assumes a transaction with a discrete, identifiable moment of exchange: a good is purchased, a service is rendered, and any defect

[3] The Digital Personal Data Protection Act, No. 22 of 2023, § 2(t) (India).

or unfairness in that exchange can be traced to a specific act by a specific seller. Data-driven commerce disrupts this model in three distinct ways. First, the "product" a consumer receives, a personalised recommendation, a targeted advertisement, a credit score, is generated continuously from an accumulating store of behavioural data rather than exchanged at a single point in time, making it considerably harder to identify the moment at which a consumer's rights were engaged or violated. Second, the party actually processing a consumer's data is frequently not the party the consumer transacted with directly, since data brokers, advertising networks and cloud infrastructure providers routinely sit behind the consumer-facing platform, diffusing accountability across a chain of processors the ordinary consumer has no visibility into. Third, the harm data misuse produces is often probabilistic and delayed, manifesting as an elevated risk of identity theft or discriminatory profiling rather than an immediate, quantifiable loss, a temporal mismatch that sits uneasily with consumer protection remedies designed around discrete, provable harm. Each of these three features recurs throughout the vulnerabilities and enforcement gaps examined later in this paper.

3. THE EVOLUTION OF DATA PROTECTION LAW: INTERNATIONAL AND INDIAN TRAJECTORIES

The legal architecture of data protection has evolved globally in response to the exponential growth of digital technology and the accelerating commodification of personal data, reflecting a gradual shift from treating privacy as an abstract civil liberty toward recognising data protection as a specific, enforceable legal right integral to consumer welfare and democratic governance. The Organisation for Economic Co-operation and Development's 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data introduced foundational principles, data minimisation, purpose limitation and accountability, that continue to inform data protection frameworks worldwide.[4] The European Union's General Data Protection Regulation, enforced from 2018, remains the most comprehensive and citizen-centric regime globally, establishing enforceable rights of access, rectification, erasure and portability, imposing privacy-by-design and privacy-by-default obligations on controllers and processors, mandating Data Protection Officers within qualifying organisations, and backing these obligations with penalties of up to four per cent of global annual turnover.[5] The United States, by contrast, follows a sectoral model lacking any unified federal statute: the Health Insurance Portability and Accountability Act governs health data, the Children's Online Privacy Protection Act governs data belonging to minors, the Gramm-Leach-Bliley Act governs financial institutions, and the California Consumer Privacy

---

4 Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

5 Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.

Act supplies the most comprehensive state-level protection, granting consumers rights to know what information is collected, to delete it, to opt out of its sale, and to receive equal service notwithstanding the exercise of these rights.[6] This sectoral approach prioritises business flexibility and innovation over the comprehensive baseline protection the European model supplies, and jurisdictions including Brazil, South Africa and China have since adopted GDPR-inspired comprehensive statutes, suggesting a broader global convergence toward rights-based data governance from which India's own reform can be situated comparatively.

India's own trajectory toward a dedicated data protection statute proceeded considerably more haltingly. For most of the digital era, data privacy existed only in the shadow of the Information Technology Act, 2000, whose Sections 43A and 72A provided narrow, weakly enforced protection, compensation for failure to protect sensitive personal data and punishment for unauthorised disclosure respectively, without either the specificity or the institutional backing a comprehensive privacy regime requires.[7] The decisive turning point arrived with the Supreme Court's unanimous nine-judge decision in Justice K.S. Puttaswamy v. Union of India, which declared the right to privacy a fundamental right under the Constitution, supplying the doctrinal foundation on which subsequent legislative reform would be built.[8] The Justice B.N. Srikrishna Committee's 2018 report and draft Personal Data Protection Bill, heavily influenced by the GDPR and introducing concepts including "data fiduciary" and "data principal" alongside a proposed Data Protection Authority, led to the Personal Data Protection Bill, 2019, which drew sustained criticism for its complexity and for the breadth of exemptions it afforded government processing, and was ultimately withdrawn in August 2022.[9] A simplified successor, the Digital Personal Data Protection Bill, 2022, followed within months and eventually matured into the Digital Personal Data Protection Act, 2023, notified on 11 August 2023, giving India its first dedicated, enforceable digital privacy statute. The Consumer Protection Act, 2019 supplies a parallel, complementary layer of protection, recognising unfair trade practices involving the misuse of consumer information particularly within e-commerce. To operationalise the 2023 Act, the Ministry of Electronics and Information Technology released the Draft Digital Personal Data Protection Rules, 2025 on 3 January 2025 for public consultation, addressing consent templates, breach-

6 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199 (US); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (US); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (US).

7 The Information Technology Act, No. 21 of 2000, §§ 43A, 72A (India).

8 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

9 Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).

reporting formats and redressal timelines, marking the transition from statutory principle to implementing procedure.

4. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 AND DRAFT RULES, 2025: STRUCTURE AND CRITICAL ASSESSMENT

The Digital Personal Data Protection Act, 2023 applies exclusively to digital personal data, information identifying an individual that is either collected in digital form or subsequently digitised, and it introduces a clear accountability structure through two defined roles: the data principal, the individual to whom the personal data relates, and the data fiduciary, any person or entity determining the purpose and means of processing that data.[10] The Act includes specific protections for children, prohibiting behavioural tracking and targeted advertising directed at minors and requiring verifiable parental or guardian consent before a minor's data may be processed, a deliberate safeguard against exploitation and data-driven manipulation of a particularly vulnerable population. To enforce these obligations, the Act establishes the Data Protection Board of India, empowered to adjudicate complaints, impose penalties for non-compliance and oversee the regime's overall functioning; the Board's eventual independence, technical capacity and accessibility will substantially determine whether the Act's protections translate into practical accountability.[11]

The Draft Digital Personal Data Protection Rules, 2025 are intended to translate these broad statutory principles into operational procedure, addressing standardised consent templates, defined timelines for fiduciaries to respond to access, correction or deletion requests, and breach-notification requirements running to both the Board and affected individuals.[12] Critical assessment of the Draft Rules, however, reveals significant gaps. Several provisions remain under-specified: the Rules require that consent be "informed and specific" without prescribing a standard format or language for consent templates, risking legally compliant but practically opaque disclosure, and they require breach notification without specifying a firm time frame comparable to the GDPR's seventy-two-hour standard or defining the severity threshold that triggers disclosure to affected data principals, an ambiguity capable of producing delayed or selective reporting in practice.[13] The consequence of this drafting choice is not merely theoretical: a fiduciary facing no fixed reporting deadline retains considerable discretion over the timing of disclosure, and that discretion is exercised, in the ordinary course, by the very entity whose commercial interest lies in minimising reputational and regulatory exposure from the breach

---

10 The Digital Personal Data Protection Act, No. 22 of 2023, § 2(i), (j) (India).
11 The Digital Personal Data Protection Act, No. 22 of 2023, ch. V (India).
12 The Draft Digital Personal Data Protection Rules, 2025 (India).
13 Id.

it is required to report, a structural conflict the Rules as drafted do not adequately address.

The Draft Rules likewise leave the Board's practical enforcement powers under-defined, offering no clear account of its investigative authority, evidence-gathering procedure, or audit powers, and no detailed methodology for calculating penalties or weighing aggravating and mitigating factors, a gap that risks inconsistent or insufficiently deterrent enforcement relative to the more developed supervisory architecture the GDPR's national authorities operate under. The absence of a codified penalty methodology is particularly consequential given the scale differential among India's data fiduciaries: a schedule of fines calibrated only loosely, without clear reference to turnover, severity or repeat conduct, risks becoming either toothless against the largest technology platforms, for whom even a substantial fixed penalty may represent a negligible cost of doing business, or disproportionately punitive against smaller fiduciaries operating with far thinner margins, undermining the compliance-with-innovation balance the Rules explicitly aim to strike.

Finally, the Rules' emphasis on ease of doing business and voluntary compliance, while understandable given India's interest in supporting a large population of smaller data fiduciaries, leaves unclear how a data principal might appeal a Board decision or seek redress beyond the Board's own administrative process, a due-process gap of real consequence for the consumer-centric framework this paper argues the Act should aspire to. Read together, these three gaps, definitional imprecision, under-specified enforcement powers, and an uncertain appellate pathway, describe a regulatory architecture that has correctly identified the categories of rule required for effective data governance without yet supplying the operational detail that turns a category into an enforceable standard.

5. CONSUMER VULNERABILITIES, DATA RIGHTS AND ENFORCEMENT CHALLENGES

Despite being the primary subjects of data collection, consumers in practice possess limited meaningful agency within the digital data ecosystem. Privacy policies are typically legalistic, lengthy and difficult to parse, producing consent that is technically obtained but substantively uninformed; once data is shared, consumers retain minimal visibility into its subsequent processing and limited practical ability to modify or delete it; the relationship between individual users and platforms is structurally asymmetrical, with corporations wielding disproportionate control over data use and retention; the sheer volume of consent prompts and pop-ups produces genuine consent fatigue, encouraging reflexive click-through behaviour rather than considered choice; and many platforms deploy "dark patterns," interface designs deliberately structured to

nudge users toward greater data disclosure or to obstruct opt-out pathways, further undermining the meaningfulness of consent as a protective mechanism.

Against this backdrop, the Act recognises a cluster of data-specific consumer rights whose practical value depends substantially on implementation. The right to information entitles consumers to know what data is collected, for what purpose, by whom, for how long, and with whom it will be shared, though the continuing complexity of most privacy disclosures means this right requires standardised, genuinely accessible disclosure formats to become meaningful in practice. The right to consent requires that consent be informed, specific, freely given and revocable, a standard the prevalence of default opt-ins and manipulative interface design continues to test in practice notwithstanding its statutory centrality. The right to data portability, permitting consumers to transfer data across platforms and thereby avoid vendor lock-in, remains constrained by the absence of clear technical standards and regulatory support for interoperability. The right to erasure allows a data principal to seek deletion of data no longer necessary for its original purpose, following consent withdrawal, or following unlawful processing, a right well developed under the GDPR but still only partially operationalised in India. The right to redressal and compensation depends on the Data Protection Board's capacity and independence, both of which remain to be tested in practice, while consumer commissions established under general consumer protection law retain only limited authority over data-specific disputes. Finally, the right against algorithmic bias and discrimination, addressing the growing use of automated decision-making in consequential consumer contexts, remains comparatively underdeveloped in Indian law relative to the GDPR's more explicit protections against automated decision-making, even as artificial intelligence systems increasingly mediate credit, insurance and employment decisions affecting Indian consumers.

These vulnerabilities are compounded by structural challenges spanning legal, technological and consumer-facing dimensions. India's data governance landscape remains split across multiple statutes and sectors, generating continuing uncertainty about which framework applies in overlapping cases, while enforcement has historically been weak, with unsolicited communication and data misuse frequently going unaddressed even as the newly constituted Data Protection Board's practical independence and authority against large technology platforms remains untested. Cross-border data flows compound the difficulty further, since many services store consumer data overseas, leaving Indian users with limited practical recourse where a breach originates outside domestic jurisdiction and international regulatory cooperation remains underdeveloped. On the technological side, artificial intelligence, the Internet of Things and machine learning evolve considerably faster than legislative and regulatory processes can track, leaving regulators perpetually working to

understand technologies that have often already been superseded by the time governing rules are finalised; cybersecurity infrastructure across public and private systems remains inconsistent, and the growing sophistication of re-identification techniques, capable of reversing anonymisation by cross-referencing ostensibly de-identified datasets against other available information, undermines the long-standing assumption that anonymisation alone is sufficient to protect privacy. On the consumer side, low digital literacy, particularly across rural and semi-urban India, compounds a digital divide that extends beyond mere access into the practical capacity to exercise legal rights, while the continuing prevalence of dark patterns and dense, jargon-heavy privacy disclosures leaves many consumers surrendering meaningful control over their data without genuine awareness of having done so.

India's documented data breach record illustrates the practical stakes of these gaps. A 2021 breach affecting Air India, arising from a cyberattack on its data processor SITA, exposed personal data belonging to 4.5 million passengers spanning a decade of records; a 2022-2023 breach at travel platform RailYatri exposed sensitive passenger information amid inconsistent official findings; the CoWIN vaccination portal was reported in 2023 to have leaked Aadhaar and passport data through a Telegram bot, prompting a security review despite official denial; a 2024-2025 breach at insurer Star Health exposed the medical data of over thirty-one million customers, accompanied by direct threats against company executives; the Diksha educational platform exposed student and teacher data through an unprotected cloud server in 2023, with no remediation for months despite prior warning; consumer electronics company boAt suffered a breach affecting 7.5 million customers in February 2024; and state telecommunications provider BSNL saw 278 gigabytes of network data, including SIM and server information, exposed in 2024.[14] The Aadhaar biometric identity system has itself been subject to repeated reported breaches since 2018, including allegations of a 2023 exposure affecting as many as 815 million Indians. These incidents, spanning aviation, healthcare, education, telecommunications and state identity infrastructure, demonstrate that the risk data protection law exists to address is neither speculative nor confined to any single sector, reinforcing the urgency of the institutional and procedural gaps identified above.

6. JUDICIAL FOUNDATIONS OF DATA PROTECTION IN INDIA

India's data protection landscape has been shaped as much by judicial interpretation as by legislation. The Supreme Court's unanimous verdict in Justice K.S. Puttaswamy v. Union of India remains the pivotal moment in this jurisprudence, affirming that the right to privacy is a fundamental right under

[14] Impacts of Data Breaches on Consumer Privacy Rights: A Comparative Analysis of Data Protection Laws in India, the EU, and the US, Amikus Qriae (2025).

the Constitution and establishing that personal data protection is a direct extension of that constitutional guarantee, a holding that supplied the doctrinal foundation for every subsequent legislative development traced in Part 3.[15] The nine-judge bench's decision is significant for present purposes not merely for its headline holding but for the proportionality framework it articulated alongside it, requiring that any state action infringing privacy satisfy tests of legality, legitimate aim and proportionality, a standard that continues to inform how courts assess data-related state action, including surveillance and biometric identification programmes, independently of whatever specific statutory scheme happens to be in force at a given time. The Court returned to this foundation in the Aadhaar reference, Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, upholding the Aadhaar scheme's core architecture by a four-to-one majority while striking down provisions permitting private-sector Aadhaar authentication and reading down the disclosure provisions of Section 33, thereby reinforcing strict limitations on data usage, purpose specification and user consent even within a constitutionally validated biometric identification programme.[16]

Read together, these decisions establish that Indian data protection law rests on a constitutional foundation independent of the statutory scheme examined in this paper, a foundation the Digital Personal Data Protection Act must be interpreted consistently with, and one capable of supplying an independent remedy where the statutory scheme itself proves insufficient. This constitutional backstop matters practically as well as doctrinally: because the right to privacy is now settled as an Article 21 guarantee, a consumer whose data has been mishandled in a manner the Digital Personal Data Protection Act's own remedial mechanisms fail to address adequately, whether because the Data Protection Board's capacity proves inadequate or because a given harm falls outside the Act's specific provisions, retains recourse to constitutional writ jurisdiction, a safety valve unavailable to consumers in jurisdictions whose privacy protection rests on statute alone.

Notwithstanding this constitutional foundation, several practical challenges continue to constrain effective enforcement. The Data Protection Board of India remains in the early stages of full operational capacity, and its ultimate independence, resourcing and capacity to manage an anticipated volume of complaints and investigations remain uncertain. Ambiguities within both the Act and the Draft Rules, examined in Part 4, risk inconsistent application across data fiduciaries and regulatory bodies, undermining the legal certainty a data protection regime is meant to supply. Public awareness of data rights remains limited across large segments of the population, meaning that statutory protections, however well drafted, may not translate into meaningful practical

---

15 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

16 Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.), (2019) 1 S.C.C. 1 (India).

empowerment absent sustained digital literacy investment. Smaller businesses face a disproportionate compliance burden relative to their scale, risking either non-compliance or a chilling effect on data-driven innovation among precisely the enterprises India's broader digital economy strategy depends upon. And the underlying tension between robust privacy protection and continued technological and economic innovation remains unresolved in the Act's present design, a tension any mature data protection regime must continue to calibrate rather than treat as settled by a single legislative enactment.

7. TOWARDS A CONSUMER-CENTRIC FRAMEWORK: FINDINGS AND RECOMMENDATIONS

The analysis in this paper yields several core findings. The Digital Personal Data Protection Act, 2023 represents a genuine advance, finally affording Indian consumers clear statutory rights of consent, correction and access over their personal data. The Draft Rules of 2025 add operationally necessary detail on consent mechanics and breach reporting, though their ultimate effectiveness depends on the strength of the enforcement architecture that accompanies them. The establishment of the Data Protection Board is a positive institutional step whose real independence and administrative readiness remain to be demonstrated in practice. The Act's specific protections for children's data reflect a thoughtful attentiveness to particularly vulnerable data subjects, and the constitutional jurisprudence flowing from Puttaswamy has been instrumental in establishing privacy as a fundamental right and in pressing successive governments toward legislative action. At the same time, real and continuing gaps persist: many consumers remain unaware of their data rights, significant statutory and regulatory provisions remain vague, enforcement mechanisms are still maturing, and smaller enterprises face a compliance burden that may prove disproportionate to their scale.

Closing these gaps requires action across several fronts. The Data Protection Board must be established as a genuinely independent, adequately funded body with clearly defined investigative and enforcement powers sufficient to act credibly against well-resourced technology platforms, rather than remaining an administratively constrained adjudicatory body in practice. Sustained, wide-reaching public awareness campaigns and digital literacy initiatives are necessary if the rights the Act confers are to translate into rights consumers actually understand and exercise, particularly across the rural and semi-urban populations for whom the digital divide extends beyond access into legal comprehension. Compliance obligations should be calibrated to enterprise scale, offering simplified pathways for smaller data fiduciaries that preserve core privacy protections without imposing disproportionate cost on India's start-up ecosystem. The ambiguities identified in Part 4, concerning consent format standards, breach-notification timelines and penalty methodology, require

detailed implementing guidance to prevent the inconsistent application that under-specified rules invariably produce. Businesses should be encouraged, through regulatory incentive as much as obligation, to build privacy protection into products by design and by default rather than treating compliance as an afterthought layered onto existing systems. Finally, sustained collaboration among government, industry, technical experts and civil society will be necessary to keep the legal framework responsive to a technological landscape that, as Part 5 demonstrates, evolves considerably faster than legislative process can track unassisted.

8. CONCLUSION

The enactment of the Digital Personal Data Protection Act, 2023, together with the Draft Rules of 2025, marks a genuine advance in India's effort to safeguard personal data and give practical effect to the constitutional right to privacy the Supreme Court recognised in Puttaswamy. The framework introduces protections, procedural clarity and institutional oversight that were absent for too long from India's digital governance landscape, reflecting an evident intent to align with global standards while remaining responsive to India's own developmental and administrative context. This progress, however, is properly understood as a foundation rather than a completed achievement. The effectiveness of India's data protection regime will ultimately depend on the strength of its enforcement, the clarity of its implementing rules, and the extent to which ordinary consumers come to understand and exercise the rights the law now affords them; absent these conditions, legal protection risks remaining substantially symbolic rather than substantive. A sustained, multi-stakeholder effort involving lawmakers, regulators, businesses and citizens alike will be required to translate the Act's statutory promise into a data protection ecosystem that is genuinely transparent, accountable and equitable, one capable of supporting continued digital innovation without treating consumer privacy as an acceptable cost of that innovation's continued growth.

BIBLIOGRAPHY

Statutes and Regulations

1. The Constitution of India, 1950, art. 21.
2. The Information Technology Act, No. 21 of 2000, §§ 43A, 72A (India).
3. The Digital Personal Data Protection Act, No. 22 of 2023, § 2 (India).
4. The Draft Digital Personal Data Protection Rules, 2025 (India).
5. The Consumer Protection Act, No. 35 of 2019 (India).
6. Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1.
7. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (US).

8. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (US).
9. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199 (US).

Cases

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
2. Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar-5J.), (2019) 1 S.C.C. 1 (India).

Reports and Secondary Sources

1. Ministry of Communications, Azadi Ka Amrit Mahotsav: Universal Connectivity and Digital India Initiatives, Press Information Bureau (Aug. 2, 2024).
2. Simon Kemp, Digital 2025: India, DataReportal (Feb. 25, 2025).
3. Organisation for Economic Co-operation and Development, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).
4. Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).
5. United Nations Guidelines for Consumer Protection (2016).