INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 7 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 7 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-7-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 7 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DATA PRIVACY AND PROTECTION IN INDIA: A CRITICAL DOCTRINAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 IN THE LIGHT OF CONSTITUTIONAL STANDARDS AND INTERNATIONAL BENCHMARKS

AUTHOR - G. MAHENDHIRA ADHITHYA* & Ms. K. KEERTHANA**

* STUDENT AT SCHOOL OF LAW, VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES (VISTAS)

** ASSISTANT PROFESSOR AT SCHOOL OF LAW, VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES (VISTAS)

BEST CITATION – G. MAHENDHIRA ADHITHYA & Ms. K. KEERTHANA**,** DATA PRIVACY AND PROTECTION IN INDIA: A CRITICAL DOCTRINAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 IN THE LIGHT OF CONSTITUTIONAL STANDARDS AND INTERNATIONAL BENCHMARKS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (7) OF 2026, PG. 13-23, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I73

ABSTRACT

The governance of personal data in India stands at a constitutionally consequential inflection point. The unanimous recognition of informational privacy as a fundamental right by a nine judge bench of the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1 imposed a proportionality calibrated constitutional mandate upon all subsequent legislative endeavor's in this domain. The Digital Personal Data Protection Act, 2023 (DPDPA), India's first purpose specific data protection statute, represents the culmination of a protracted and politically contested legislative process. This article undertakes a rigorous doctrinal analysis of the DPDPA 2023, situating it within the constitutional architecture erected by the Puttaswamy jurisprudence and evaluating it against the normative standards established by the European Union's General Data Protection Regulation (GDPR). The analysis reveals that while the Act constitutes a genuine legislative advance, it is marred by structural deficiencies of constitutional significance: the sweeping executive exemption under Section 17(2) fails the proportionality standard; the Data Protection Board's dependence on executive appointment compromises institutional independence; the omission of rights to data portability and protection against automated decision making leaves critical lacunae; and the whitelist based cross border transfer mechanism substitutes diplomatic pragmatism for objective adequacy review. Drawing on comparative frameworks from the European Union and the United Kingdom, and examining the practical dimensions of enforcement deficits, surveillance accountability gaps, and the emerging challenge of algorithmic governance, this article advances a programme of legislative, institutional, and policy reforms directed at aligning India's data protection framework with its constitutional aspirations.

Keywords: Data Privacy; Digital Personal Data Protection Act 2023; Informational Self Determination; Proportionality Doctrine; GDPR; Data Protection Board; Surveillance; Algorithmic Decision Making; Constitutional Rights; Comparative Data Law.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 7 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

I. INTRODUCTION

The emergence of personal data as the preeminent economic and political resource of the twenty first century has compelled legal systems across the globe to reckon with a regulatory challenge of unprecedented complexity. In India, this challenge carries a distinctive constitutional dimension: with over 800 million internet users, a pervasive government run biometric identity infrastructure, and a rapidly expanding data intensive economy, the country simultaneously generates some of the largest volumes of personal data in the world and confronts some of the acutest risks of its misappropriation. The structural asymmetry between technologically sophisticated data fiduciaries and largely uninformed data subjects creates conditions in which the unregulated exercise of informational power threatens not merely commercial fairness but the constitutional conditions for individual autonomy and democratic participation.

India's regulatory response to this challenge has historically been reactive and fragmented. The Information Technology Act, 2000 (IT Act), augmented by the Sensitive Personal Data or Information Rules of 2011 (SPDI Rules), provided a compensation oriented framework applicable exclusively to private body corporates, leaving government data processing entirely unregulated and failing to establish any substantive rights of data subjects. The constitutional watershed arrived on 24 August 2017, when the Supreme Court's nine judge bench in *Puttaswamy* definitively recognised the right to privacy including informational privacy as a fundamental right under Article 21, and constitutionally mandated the enactment of a data protection regime consonant with proportionality principles. After a gestation extending across multiple Bills, parliamentary committee reviews, and public consultations, Parliament enacted the Digital Personal Data Protection Act, 2023, which received Presidential assent on 11 August 2023.

This article argues that the DPDPA 2023, despite representing a genuine and overdue legislative advance, fails in critical respects to satisfy the constitutional standard of proportionality established by *Puttaswamy* and falls materially short of the international benchmarks exemplified by the GDPR. Section II establishes the conceptual and theoretical framework. Section III provides a legal analysis of the constitutional and statutory architecture. Section IV identifies critical structural gaps. Section V analyses the relevant case law and regulatory dimensions. Section VI examines recent developments including surveillance concerns and AI governance. Section VII advances a programme of reform recommendations. Section VIII concludes.

II. CONCEPTUAL AND THEORETICAL FRAMEWORK

Privacy, as a juridical concept, resists monosemic definition. Its theoretical genealogy encompasses Warren and Brandeis's foundational articulation in 1890 of the right "to be let alone," Alan Westin's control based conception of privacy as the individual's claim to determine the terms on which information about oneself is communicated to others, Ruth Gavison's tripartite formulation grounded in secrecy, anonymity, and solitude, and Helen Nissenbaum's sophisticated theory of contextual integrity, which locates privacy violations not in the quantum of information disclosed but in the appropriateness of information flows relative to their governing social norms. Each of these theoretical traditions contributes an essential dimension to the analysis of data protection law, and collectively they illuminate the inadequacy of any purely technical or security focused approach to the regulation of personal data.

The concept of informational self determination, originating in the German

Federal Constitutional Court's landmark 1983 Census Judgment (*Volkszählungsurteil*, BVerfGE 65, 1), constitutes the most jurisprudentially significant theoretical contribution to contemporary data protection law. The Court held that the right to informational self determination the individual's constitutionally guaranteed capacity to determine the informational image that others form of them is grounded in the foundational guarantee of human dignity and the right to free development of personality. This formulation transformed data protection from a regulatory technicality into a dimension of constitutional freedom, providing the normative bridge between abstract privacy rights and the concrete architecture of data protection legislation. Its influence permeates the GDPR's rights based framework and has been incorporated, through the *Puttaswamy* judgment, into Indian constitutional law.

Data protection, as distinct from privacy, denotes the body of regulatory law and institutional practice that governs the collection, processing, storage, transfer, and use of personal information. Scholars including Paul De Hert and Serge Gutwirth have articulated the conceptual distinction with precision: privacy functions as a "shield" that protects individuals from unwanted intrusion, while data protection operates as a "tool" that enables the transparent, accountable, and lawful management of data. The DPDPA 2023 adopts a data protection paradigm premised on seven foundational principles lawful and fair processing, purpose limitation, data minimisation, accuracy, storage limitation, security, and accountability principles that closely mirror the GDPR's architecture and reflect a deliberate alignment with international normative standards.

Proportionality, the third foundational concept of this analysis, serves as the constitutional bridge between privacy theory and legislative assessment. As articulated by the Supreme Court in *Puttaswamy*, any state action curtailing the right to informational privacy must satisfy a fourfold test: the restriction must be prescribed by a sufficiently precise and foreseeable law; it must pursue a legitimate aim; it must be rationally connected to and necessary for that aim; and it must constitute the least restrictive means available. This standard closely analogous to the proportionality analysis employed by the European Court of Human Rights and the Court of Justice of the European Union provides the normative grammar within which the DPDPA 2023 must be constitutionally evaluated.

III. LEGAL ANALYSIS: CONSTITUTIONAL AND STATUTORY ARCHITECTURE

The constitutional framework of data privacy in India is anchored principally in Articles 21 and 19 of the Constitution of India, 1950, read through the interpretive prism of six decades of Supreme Court jurisprudence. The transformative interpretation of Article 21 commenced with *Maneka Gandhi v. Union of India* (1978) 1 SCC 248, in which the Court held that the procedure established by law depriving a person of life or personal liberty must be "right, just and fair," thereby importing a substantive due process dimension that opened Article 21 to a broad spectrum of unenumerated rights. The application of this interpretive methodology to informational privacy proceeded through a series of decisions *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (declining to recognize a constitutional right to privacy); *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (recognizing a spatial dimension of personal liberty while formally denying a right to privacy); *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148 (acknowledging a qualified right to privacy as an emanation of Articles 19 and 21); and *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301 (extending privacy protection to telephonic communications and recognizing its chilling effect on freedom of expression) before the doctrinal ambiguity was definitively resolved by *Puttaswamy* in 2017.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 7 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The *Puttaswamy* judgment constitutes a constitutional watershed of the first order. The nine judge bench unanimously overruled *M.P. Sharma* and *Kharak Singh* to the extent that they denied a constitutional right to privacy, and affirmed privacy as a fundamental right inhering in personhood, encompassing spatial, decisional, and informational dimensions. Justice D.Y. Chandrachud's plurality opinion which carries the greatest doctrinal weight for data protection law explicitly identified "informational privacy" as a constitutional entitlement protecting individuals against the "unauthorized use of personal information," grounded the constitutional right in the twin values of human dignity and individual liberty, and directed the Union Government to enact a data protection regime consonant with constitutional values. In doing so, the Court effectively constitutionalized the foundational principles of modern data protection law: purpose limitation, data minimization, necessity, and accountability.

India's statutory data protection framework has evolved through three distinct legislative phases. The IT Act 2000, modelled on the UNCITRAL Model Law on Electronic Commerce, was designed primarily to facilitate e commerce and digital governance rather than to protect personal data. Its data protection provisions principally Section 43A, inserted by the 2008 Amendment, which imposes civil liability on body corporates for negligent handling of sensitive personal data, and Sections 66C and 66E, creating criminal offences for identity theft and privacy violations are peripheral to the Act's commercial purpose and suffer from profound structural deficiencies. They apply exclusively to private body corporates, entirely exempting government data processing; they adopt a negligence based compensatory approach rather than a rights based protective framework; they lack an independent supervisory mechanism; and they do not establish substantive data subject rights including access, correction, portability, or erasure.

The SPDI Rules 2011, promulgated under the IT Act, represented a modest operational advance but perpetuated the same fundamental inadequacies. The definition of sensitive personal data is simultaneously over inclusive and under inclusive, omitting emerging categories such as genetic data, location data, and political opinions. The consent mechanism requiring consent "in writing through letter or fax or email" lacks the granularity and meaningfulness necessary to operationalize informational self determination. Most critically, the Rules share the IT Act's structural asymmetry: the largest and most powerful data processor in India the government operates entirely outside the regulatory framework, a position constitutionally untenable in the post *Puttaswamy* landscape.

The DPDPA 2023 constitutes a paradigmatic shift in India's data governance architecture. Enacted following a legislative process spanning the Srikrishna Committee Report (2018), the Personal Data Protection Bill 2019, Joint Parliamentary Committee review, parliamentary withdrawal of the 2019 Bill, and redrafting, the Act establishes a principles based framework for the processing of digital personal data. Its principal innovations include: the introduction of the data fiduciary/data principal conceptual architecture; the recognition of data principal rights to access, correction, erasure, and grievance redressal; the imposition of comprehensive obligations on data fiduciaries including data minimization, purpose limitation, and security safeguards; and the creation of the Data Protection Board of India as a dedicated adjudicatory authority with power to impose financial penalties of up to ₹250 crore for specified violations.

IV. CRITICAL ISSUES AND STRUCTURAL GAPS

The DPDPA 2023's structural deficiencies are both numerous and constitutionally significant. Four merit particular analytical attention: the breadth of the government exemption under Section 17(2); the institutional dependence of the Data Protection Board; the

incompleteness of data subject rights; and the architecture of cross border data transfer governance.

Section 17(2) of the Act empowers the Central Government, by notification, to exempt any instrumentality of the state from the application of any or all provisions of the Act in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order, or prevention of incitement to any cognizable offence. This provision is constitutionally suspect on multiple grounds. First, the exemption grounds, while tracking the language of Article 19(2), are drafted at a level of generality that provides insufficient precision to satisfy the legality requirement of the *Puttaswamy* proportionality standard: a legislative provision authorizing the executive to impose limitations on fundamental rights must define the scope of those limitations with sufficient clarity and foreseeability. Section 17(2)'s open ended delegation fails this requirement. Second, the provision permits blanket exemption of entire government instrumentalities from all provisions of the Act, including those relating to security safeguards protecting data subjects against breach a breadth that is difficult to justify as the least restrictive means of achieving the specified aims. Third, the absence of any judicial or independent oversight mechanism for the exercise of the exemption power contravenes the internationally recognized principle that limitations on data protection rights for national security or law enforcement purposes must be subject to effective judicial review, a principle reflected in the GDPR framework and the jurisprudence of the European Court of Human Rights.

The institutional design of the Data Protection Board raises equally serious concerns regarding regulatory independence. The Act vests appointment of the Chairperson and Members entirely in the Central Government, without specifying qualifications for appointment, establishing fixed terms of office, or providing for security of tenure. These omissions are inconsistent with the principles of regulatory independence articulated by the Supreme Court in *R. Gandhi v. Union of India*, (2010) 11 SCC 1, and with the GDPR's requirement that supervisory authorities be "fully independent" public authorities whose members enjoy "freedom from external influence." A Board whose members owe their appointment to the Central Government confronts structural pressures whether explicit or implicit that compromise its capacity for impartial adjudication, particularly in cases involving government data processors. This structural dependence is especially problematic given that the constitutional obligation to protect the right to informational privacy runs against both state and non state actors.

The rights framework established by the DPDPA 2023, while representing a significant advance over the rights free environment of the IT Act, falls short of internationally recognized standards in several respects. The Act does not include a right to data portability, enabling individuals to receive their data in a structured, machine readable format suitable for transfer to an alternative data fiduciary a right that promotes competitive markets and operationalizes data subject autonomy. It does not include a right to object to automated decision making with significant effects: as algorithmic systems proliferate across India's financial services, insurance, and government welfare sectors, the absence of an equivalent to the GDPR's Article 22 protection may have severe practical consequences for data subjects. The Act also does not include a right to restrict processing in specified circumstances, nor does it impose a general accountability obligation requiring data fiduciaries to demonstrate compliance an absence that may limit the effectiveness of the Board's supervisory function.

The cross border data transfer regime under Section 16 adopts a government whitelist approach, under which the Central Government

designates the countries to which personal data may be transferred following an assessment of unspecified relevant factors. This approach differs fundamentally from the GDPR's adequacy mechanism, under which the European Commission must determine that a recipient country's data protection framework provides substantively equivalent protections a determination subject to judicial review by the Court of Justice of the European Union, as demonstrated in *Data Protection Commissioner v. Facebook Ireland* (Schrems II), Case C-311/18. By substituting executive designation for objective adequacy review, Section 16 creates the risk that countries are approved for data transfer on diplomatic or economic grounds rather than on the basis of the level of protection they afford to Indian data subjects.

V. CASE LAW AND REGULATORY ANALYSIS

The judicial architecture of Indian data protection law was constructed across five decades of Supreme Court jurisprudence culminating in the *Puttaswamy* judgment. *Kharak Singh*'s formalist majority which declined to recognize a constitutional right to privacy while implicitly acknowledging a spatial dimension of personal liberty established the doctrinal tension between textual fidelity and constitutional purposivism that would animate privacy jurisprudence for the following half century. Justice Subba Rao's dissent in *Kharak Singh*, articulating liberty as encompassing "freedom from encroachments on private life," planted the conceptual seed from which a more robust doctrine would eventually grow. *Gobind*'s recognition of a qualified right to privacy as a "penumbral right" of guaranteed freedoms, grounded in American substantive due process doctrine and Vestinian privacy theory, advanced the jurisprudential project while simultaneously undermining it by upholding the challenged surveillance regulation. *PUCL*'s recognition that telephonic surveillance violates both Article 21 and Article 19(1)(a) and that unchecked state interception creates a chilling effect on freedom of expression established the critical doctrinal link between informational privacy and the broader landscape of constitutional freedoms.

The *Puttaswamy* judgment of 2017 achieved the definitive resolution of six decades of doctrinal ambiguity. The Court's recognition of privacy as a natural right "inhering in personhood," its grounding of informational privacy in the values of human dignity and individual autonomy, its explicit direction to the Union Government to enact a data protection regime, and its articulation of the proportionality standard as the constitutional measure for evaluating limitations on the right collectively created the normative architecture within which the DPDPA 2023 must be assessed. The second *Puttaswamy* judgment of 2019 addressing the Aadhaar scheme demonstrated that this proportionality architecture has practical constitutional bite, striking down Section 57 of the Aadhaar Act (permitting private entity authentication) and provisions mandating Aadhaar linkage with bank accounts and mobile connections as disproportionate, while upholding the core architecture of the scheme.

From a regulatory standpoint, the DPDPA 2023 represents India's first attempt at comprehensive statutory data protection, but its enforcement architecture raises serious concerns. The Data Protection Board is constituted as a purely digital adjudicatory mechanism proceedings are conducted electronically without physical hearings an innovation that may enhance efficiency but raises access to justice concerns for data principals without digital literacy or internet connectivity. The principle of universal access to justice, recognized as a constitutional value in *Anita Kushwaha v. Pushap Sudan*, (2016) 8 SCC 509, demands that quasi judicial processes remain accessible to all, including the digitally excluded. The Act's category of "Significant Data Fiduciaries" (SDFs), designated by the Central Government based on data volume, sensitivity, and systemic risk, imposes additional obligations including mandatory Data Protection Officers, independent data audits,

and Data Protection Impact Assessments provisions broadly analogous to the GDPR's high risk processing framework but the designation power's residence in the executive rather than the independent Board raises concerns about consistency and potential political motivation.

The comparative regulatory landscape furnishes instructive lessons. The GDPR's supervisory architecture requiring genuinely independent national data protection authorities with defined appointment qualifications, fixed terms, security of tenure, financial autonomy, and investigative and sanctioning powers up to four percent of global annual turnover has demonstrably produced a deterrence effect that compensatory civil liability frameworks cannot replicate. The Irish Data Protection Commission's €1.2 billion fine imposed on Meta Platforms in 2023 illustrates the capacity of an adequately independent and resourced supervisory authority to hold even the most powerful data processors accountable. The United Kingdom's experience post Brexit obtaining an EU adequacy decision in 2021 on the basis of the substantial equivalence of its GDPR derived framework demonstrates that regulatory alignment with international standards yields tangible economic benefits by facilitating data flows without the transaction costs of alternative transfer mechanisms.

VI. RECENT DEVELOPMENTS: SURVEILLANCE, DATA BREACHES, AND ALGORITHMIC GOVERNANCE

Three categories of recent development illuminate the practical urgency of the structural reforms this article advocates: large scale data breaches, state surveillance accountability deficits, and the emerging challenge of algorithmic governance.

India has witnessed a series of significant data breaches that expose the inadequacy of the pre DPDPA regulatory framework. The Aadhaar data leak of January 2018 in which demographic data of over one billion enrolled individuals was reportedly accessible through an unauthorized government portal and subsequently through messaging platform channels exposed the structural vulnerability of centralized biometric data infrastructure in the absence of mandatory breach notification obligations or an independent supervisory authority with investigative powers. The Cowin portal breach of June 2023 in which personal health data including names, Aadhaar numbers, and vaccination status of COVID 19 registrants was reportedly accessible via a Telegram bot similarly exposed the risks of large scale government managed health databases without commensurate security oversight. While the DPDPA 2023's mandatory breach notification obligation under Section 8(6) represents a significant regulatory advance, its effectiveness will depend critically on the timelines established in implementing rules and the investigative capacity of the Data Protection Board.

The intersection of state surveillance and data privacy presents India's most acute constitutional challenge in the data protection domain. India's surveillance architecture principally governed by Section 5(2) of the Indian Telegraph Act, 1885 and the IT Act's interception provisions operates in an environment of limited legal transparency, executive self authorization, and minimal independent oversight. The Pegasus surveillance controversy of 2021, in which credible reports by the Forbidden Stories consortium and Amnesty International's Security Lab alleged the use of NSO Group's Pegasus spyware against journalists, activists, lawyers, and political figures in India, exposed the near total absence of accountability mechanisms for sophisticated state surveillance. The Supreme Court's technical committee in *Manohar Lal Sharma v. Union of India*, Writ Petition (Criminal) No. 314 of 2021, could not conclusively determine whether Pegasus had been deployed by the Indian government, partly due to insufficient cooperation from state authorities. The DPDPA

2023's Section 17 exemptions effectively place the surveillance apparatus outside the Act's accountability framework, rendering the constitutional protections of *Puttaswamy* practically unenforceable in this domain without dedicated surveillance reform legislation.

The proliferation of artificial intelligence and algorithmic decision making across India's financial, insurance, employment, and government welfare sectors generates data protection risks that the DPDPA 2023 addresses in only a nascent and indirect manner. Machine learning systems trained on large personal data sets infer sensitive information from ostensibly non sensitive inputs, produce automated decisions with significant effects on individuals, and embed structural biases that are opaque to both affected data subjects and regulatory supervisors. The absence from the DPDPA 2023 of provisions governing algorithmic transparency, automated decision making rights, or AI specific Data Protection Impact Assessments creates a regulatory lacuna that will become increasingly consequential as these systems penetrate more deeply into everyday life. India's position as a major global market for AI services and the government's own deployment of algorithmic systems in welfare allocation and law enforcement makes this gap particularly urgent.

VII. REFORMS AND RECOMMENDATIONS

A credible programmed of legislative, institutional, and policy reform must address the DPDPA 2023's structural deficiencies in a systematic and constitutionally principled manner. The following recommendations are advanced with reference to the proportionality standard of *Puttaswamy* and the comparative lessons of the GDPR and UK frameworks.

The most urgent legislative priority is the amendment of Section 17(2) to replace the current open ended executive exemption with a narrowly drawn framework that: specifies the precise conditions under which exemptions may be granted; limits exemptions to particular provisions of the Act that genuinely conflict with the specified ground, rather than permitting blanket exclusion; mandates that exemptions be time limited and subject to periodic parliamentary review; and establishes an independent judicial oversight mechanism for exemption decisions. Such modifications are constitutionally necessary to satisfy the legality and necessity requirements of the *Puttaswamy* proportionality standard and would bring India's exemption framework into alignment with the GDPR's approach to national security and law enforcement carve outs.

The DPDPA 2023 should be amended to extend its scope to non digital personal data. The present limitation to digital data creates an anomalous regulatory gap in a country where significant volumes of sensitive personal information including paper based health records, financial files, and court documentation remain in non digital form. Comprehensive data protection demands medium neutral application of its foundational principles and data subject rights.

Three additional data subject rights merit statutory incorporation: a right to data portability in structured, interoperable, machine readable format; a right to object to and seek human review of automated decisions producing significant effects; and a right to restrict processing in specified circumstances. These rights are central to the GDPR's empowerment framework and to the operationalization of informational self determination in a data intensive economy.

Structural independence of the Data Protection Board must be legislatively secured through: specified qualification requirements for Chairperson and Members emphasizing legal expertise, technical knowledge, and civil society representation; fixed terms of five years renewable once, with removal exclusively on specified grounds of incapacity or misconduct following independent inquiry; financial autonomy through appropriation from the Consolidated Fund of India; and a three year

cooling off period for former government officials involved in data processing. These safeguards are necessary to give effect to the constitutional obligation to protect the right to informational privacy against both state and private sector violations.

Dedicated surveillance reform legislation separate from but complementary to the DPDPA 2023 is an essential element of any credible data protection framework. Such legislation should specify the categories and grounds of permissible surveillance, require prior judicial authorization or independent oversight in all but the most urgent cases, establish notification obligations to affected individuals following the conclusion of surveillance operations, and provide enforceable remedies for unlawful interception. India remains one of the few major constitutional democracies without a dedicated surveillance reform statute, a lacuna that is constitutionally indefensible in the light of *Puttaswamy*'s proportionality mandate.

At the policy level, India should pursue a medium term objective of obtaining an adequacy determination from the European Commission. Achieving adequacy requiring that the DPDPA framework provide substantively equivalent protection to the GDPR would eliminate the transaction costs of alternative transfer mechanisms for EU India data flows, signal India's commitment to global data governance standards, and create a powerful external incentive for continued domestic regulatory improvement. The legislative and institutional reforms recommended in this article would, if implemented, materially advance India's prospects of adequacy recognition. Finally, the Data Protection Board should be given a statutory mandate to develop and implement a comprehensive public awareness and digital literacy programmed, targeted specifically at rural populations, elderly individuals, and other groups with limited digital access the populations for whom the gap between statutory rights and practical empowerment is most acute

VIII. CONCLUSION

India stands at a decisive juncture in the governance of personal data. The constitutional foundation for robust data protection is firmly established by the *Puttaswamy* judgment's recognition of informational privacy as a fundamental right and its articulation of the proportionality standard as the constitutional measure of legislative validity in this domain. The DPDPA 2023 represents a genuine and overdue legislative advance establishing India's first principles based, rights oriented data protection framework but it falls materially short of both the constitutional standard it must satisfy and the international benchmarks against which it will be evaluated.

The Act's structural deficiencies the disproportionately broad government exemption under Section 17(2), the institutionally dependent Data Protection Board, the incomplete rights framework, the executive controlled cross border transfer mechanism, and the absence of surveillance reform and AI governance provisions are not merely technical legislative imperfections. They represent a systematic subordination of the rights of data principals to the operational interests of government and the commercial interests of industry, a resolution of competing interests that is constitutionally questionable and normatively unsatisfying. The analytical framework established in this article grounded in *Puttaswamy*'s proportionality doctrine and calibrated against GDPR benchmarks provides the doctrinal and comparative tools for subjecting these deficiencies to rigorous constitutional scrutiny.

Data is the medium through which citizens exercise their fundamental freedoms in the digital age the freedom to communicate, associate, access information, participate in democratic processes, and determine the course of their own lives. A data protection framework that subordinates the constitutional right to informational privacy to executive discretion and commercial convenience is not

merely a regulatory shortcoming; it is an abdication of the constitutional duty to protect the conditions for the exercise of freedom. The aspiration of informational self determination articulated in Germany's Census Judgment of 1983, affirmed in India's *Puttaswamy* judgment of 2017, and given imperfect statutory expression in the DPDPA 2023 can be fully realized only through the legislative, institutional, and policy reforms this article has sought to articulate and justify.

REFERENCES

A. Primary Sources

Constitution of India, 1950, Articles 19, 21.

Information Technology Act, 2000 (No. 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 [SPDI Rules].

Digital Personal Data Protection Act, 2023 (No. 22 of 2023).

Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

Right to Information Act, 2005.

Indian Telegraph Act, 1885, s 5(2).

European Union, General Data Protection Regulation (Regulation (EU) 2016/679) [GDPR].

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108, 1981; Convention 108+, 2018).

UK General Data Protection Regulation (Retained Regulation (EU) 2016/679) and Data Protection Act 2018.

B. Case Laws

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

Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar Judgment), (2019) 1 SCC 1.

Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.

Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148.

People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

M.P. Sharma v. Satish Chandra, AIR 1954 SC 300.

R. Gandhi v. Union of India, (2010) 11 SCC 1.

Anita Kushwaha v. Pushap Sudan, (2016) 8 SCC 509.

Manohar Lal Sharma v. Union of India, Writ Petition (Criminal) No. 314 of 2021.

Data Protection Commissioner v. Facebook Ireland, Case C-311/18, [2020] ECLI:EU:C:2020:559 (CJEU, Schrems II).

Bundesverfassungsgericht, Census Act Case (Volkszählungsurteil), BVerfGE 65, 1 (1983).

Griswold v. Connecticut, 381 U.S. 479 (1965).

C. Books and Articles

Gautam Bhatia, The Transformative Constitution (HarperCollins India, 2019).

Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power' in E Claes, A Duff and S Gutwirth (eds), Privacy and the Criminal Law (Intersentia, 2006).

Lilian Edwards, 'Data Protection: Enter the General Data Protection Regulation' in Lilian Edwards (ed), Law, Policy and the Internet (Hart Publishing, 2019).

Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421.

Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2014).

Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press, 2010).

Usha Ramanathan, 'A Unique Identity Bill' (2010) 45(35) Economic and Political Weekly 10.

Paul M. Schwartz and Daniel J. Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814.

Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

Alan F. Westin, Privacy and Freedom (Atheneum, 1967).

D. Reports and Official Sources

Justice B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology, Government of India, 2018).

Joint Parliamentary Committee on the Personal Data Protection Bill, 2019, Report of the Joint Committee on the Personal Data Protection Bill (Lok Sabha Secretariat, December 2021).

Ministry of Electronics and Information Technology, Digital Personal Data Protection Bill, 2023: Draft for Public Consultation (Government of India, 2022).

Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679 (European Commission, 2018).

Amnesty International / Forbidden Stories, Pegasus Project: Forensic Methodology Report (Amnesty International Security Lab, July 2021).

INSTITUTE OF LEGAL EDUCATION

(Managed by L TO J LAW ASSOCIATES)

NO. 08, ARUL NAGAR, SEERA THOPPU,
MARUDHAANDA KURICHI, SRIRANGAM - 620102,
TAMILNADU, INDIA.

ISSN 2583-2344