INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

DIGITAL PERSONAL DATA PROTECTION IN INDIA: BALANCING PRIVACY, INNOVATION AND STATE INTERESTS

AUTHORED BY - DR PRADNYA YADAV[1]

Abstract

Personal data has quietly become one of the most valuable resources in the modern economy. Artificial intelligence, e-commerce, digital public infrastructure and data-driven governance all run on it, but the same processing that fuels growth also exposes individuals to profiling, discrimination and surveillance. In India, that tension took on constitutional weight once the Supreme Court, in Justice KS Puttaswamy (Retd) v Union of India, recognised privacy as a fundamental right and set the stage for a dedicated data protection law. The Digital Personal Data Protection Act 2023 ("DPDP Act") and the Digital Personal Data Protection Rules 2025 ("DPDP Rules") are the result.

This article looks at that framework through the lens of three interests that do not always pull in the same direction: individual privacy, technological innovation, and the State's own claims on personal data. It works through the DPDP Act's core architecture, Data Principals and Data Fiduciaries, consent and legitimate uses, individual rights, children's data, Significant Data Fiduciaries, cross-border transfers, and the Data Protection Board of India and pays particular attention to how far governmental exemptions extend and what that means for State access to personal information. The argument advanced here is that the statute is a genuine foundation, but not yet a sufficient one: whether it actually protects privacy will turn on proportionality, institutional independence, transparency, judicial oversight and real remedies, not on the text alone. The article closes with a set of proposals for a data governance model that takes both rights and innovation seriously.

Keywords: Digital Personal Data Protection Act, 2023; Privacy; Data Protection; Artificial Intelligence; Data Fiduciary; Data Principal; State Surveillance; Digital Governance; Innovation; Constitutional Rights.

[1] Assistant Professor, DES Shri Navalmal Firodia Law College, Pune.

ISSN: 2582-6433

- **Introduction**

Personal data has become an essential component of modern digital society. Online banking, digital healthcare, e-commerce, social networking, education platforms, telecommunications, digital identity systems and artificial intelligence applications depend upon the collection and processing of enormous quantities of information relating to individuals. Data can facilitate economic growth, improve public services and enable innovation; however, the same data can also be used for profiling, behavioural manipulation, discrimination, surveillance and commercial exploitation. The central legal question is therefore not whether personal data should be processed, but under what conditions such processing should be permitted and what safeguards should govern it. This question assumes particular importance in India because of the country's rapidly expanding digital economy and extensive use of digital technologies in public administration. The constitutional foundation for privacy protection was substantially strengthened by the Supreme Court's nine-judge Bench decision in *Justice KS Puttaswamy (Retd) v Union of India*. The Court unanimously recognised privacy as a constitutionally protected right arising primarily from Article 21 and other fundamental freedoms. Privacy was understood not merely as protection from physical intrusion but as encompassing dignity, autonomy, informational control and the ability of individuals to make decisions concerning their personal lives.[2] The judgment consequently altered the legal landscape concerning personal information. The Court recognised that informational privacy is an essential component of individual autonomy and that State interference with privacy must satisfy constitutional requirements.[3]

The Digital Personal Data Protection Act 2023 was enacted against this constitutional background. The legislation seeks to regulate the processing of digital personal data while recognising both the right of individuals to protect their personal data and the need to process such data for lawful purposes. The Digital Personal Data Protection Rules 2025 subsequently supplied the detailed implementation framework. The Rules were notified on 13 November 2025, with different provisions becoming operational at different stages.[4] The principal challenge for Indian data protection law is therefore to establish an equilibrium between three interests: individual privacy, technological and economic innovation, and legitimate State

[2] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, paras 24, 40, 168–169 (recognising privacy, dignity, autonomy and informational privacy).
[3] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1; see also Constitution of India, arts 14, 19 and 21.
[4] Digital Personal Data Protection Act 2023, long title and ss 4–6.

ISSN: 2582-6433

interests. An excessively restrictive framework could impede innovation and digital economic development, whereas an excessively permissive regime could undermine constitutional privacy and individual autonomy. This article critically examines whether the present framework achieves an appropriate balance and identifies areas requiring stronger institutional and constitutional safeguards.

• Constitutional Foundation of Data Privacy in India

➢ Privacy as a Fundamental Right

Prior to *Puttaswamy*, Indian constitutional jurisprudence contained an evolving but sometimes inconsistent approach to privacy. The nine-judge Bench decisively settled the issue by holding that privacy is a fundamental right protected by the Constitution.[5] The Court connected privacy with dignity, liberty and autonomy. Justice Chandrachud observed that privacy includes the preservation of personal intimacies, family life, marriage, procreation and the home, while also encompassing informational control.[6] The recognition of informational privacy is particularly relevant in the digital age. Individuals continuously generate data through their online activities. Location information, browsing histories, financial transactions, biometric identifiers and communications may collectively reveal highly intimate characteristics of an individual. Accordingly, data protection is not merely a matter of commercial regulation. It is closely connected with constitutional liberty.

➢ The Proportionality Requirement

The Supreme Court has subsequently developed proportionality as an important constitutional standard for restrictions on fundamental rights. In *K.S. Puttaswamy (Retd) v Union of India (Aadhaar)*, the Court examined State collection and use of personal information through the framework of legality, legitimate State aim and proportionality.[7] The proportionality principle requires that an interference with privacy have a legal basis, pursue a legitimate objective and maintain a rational and proportionate relationship between the objective and the means adopted. This principle should remain central to interpretation of the DPDP framework, particularly where personal data is processed by public authorities.

[5] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[6] ibid.
[7] K.S. Puttaswamy (Retd) v Union of India (2019) 1 SCC 1, especially the proportionality analysis concerning State collection and use of personal information.

ISSN: 2582-6433

- **Evolution of India's Data Protection Framework**

India's initial approach to data protection relied principally upon the Information Technology Act 2000 and subordinate rules. Section 43A of the Information Technology Act created liability relating to failure to implement reasonable security practices in relation to sensitive personal data, while the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 provided additional requirements.[8] However, this framework was inadequate for a data-driven economy. It did not establish a comprehensive rights-based regime covering the entire lifecycle of personal data. The Supreme Court's recognition of privacy in *Puttaswamy* created pressure for legislative reform. The Justice BN Srikrishna Committee subsequently proposed a comprehensive data protection framework. The legislative process ultimately resulted in the Digital Personal Data Protection Act 2023.[9] The DPDP Act adopts a comparatively streamlined structure. Rather than replicating every feature of the European General Data Protection Regulation ('GDPR'), it establishes a framework centred on lawful processing, consent, specified purposes, organisational accountability and individual rights. The DPDP Rules 2025 provide operational details concerning notice, consent, security safeguards, breach notification, children's data, Significant Data Fiduciaries, grievance redressal and other matters.

- **Core Features of the Digital Personal Data Protection Act 2023**

➢ **Data Principal and Data Fiduciary**

The Act uses the terms **Data Principal** and **Data Fiduciary**. A Data Principal is the individual to whom personal data relates, while a Data Fiduciary is the person who determines the purpose and means of processing personal data.[10] The terminology reflects a shift from treating individuals merely as sources of data towards recognising them as rights-bearing participants in the data ecosystem. The distinction is significant because responsibility is placed upon the Data Fiduciary rather than solely upon the individual. Organisations processing personal data must therefore establish systems for lawful processing, security and compliance.

➢ **Consent and Notice**

Consent constitutes an important basis for processing personal data. The Act requires consent

[8] Information Technology Act 2000, s 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.
[9] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1; Committee of Experts under the Chairmanship of Justice B N Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).
[10] Digital Personal Data Protection Act 2023, s 2.

ISSN: 2582-6433

to be free, specific, informed and unambiguous, involving clear affirmative action.[11] The notice requirement is equally significant because meaningful consent requires information. The Rules seek to strengthen transparency by requiring notices to communicate relevant information in a clear and understandable manner. However, a major practical difficulty remains: formal consent does not always constitute meaningful choice. Digital platforms frequently operate through lengthy terms and conditions, while users may have little realistic bargaining power. Consequently, Indian data protection law should increasingly focus on substantive fairness rather than treating consent as a purely formal mechanism.

- **Rights of Data Principals**

The Act provides Data Principals with several rights, including rights relating to access to information, correction and erasure of personal data, grievance redressal and nomination.[12] These rights contribute to informational self-determination. They enable individuals to exercise a degree of control over information concerning them. The effectiveness of these rights, however, depends upon accessibility. Rights that require complex procedures, technical knowledge or substantial time may be practically unavailable to ordinary citizens. Therefore, awareness and simple grievance mechanisms are essential components of meaningful data protection.

• Protection of Children and Vulnerable Data Principals

Children occupy a particularly vulnerable position within the digital environment. Online platforms can collect behavioural information from children and use it for profiling, targeted advertising or algorithmic recommendations. The DPDP Act therefore imposes additional obligations concerning children's personal data, including requirements relating to verifiable parental consent and restrictions on certain forms of processing.[13] The Rules provide further operational requirements concerning children's data. The regulatory approach is justified because children may lack the maturity necessary to understand long-term consequences of data disclosure. Nevertheless, implementation must balance protection with children's legitimate access to education, communication and digital services. A rigid verification system could create excessive identification requirements and inadvertently generate additional data

[11] Digital Personal Data Protection Act 2023, s 6.
[12] Digital Personal Data Protection Act 2023, ss 11–15.
[13] Digital Personal Data Protection Act 2023, s 9; Digital Personal Data Protection Rules 2025, provisions concerning children's personal data.

ISSN: 2582-6433

collection. Consequently, child protection mechanisms should follow the principle of data minimisation and avoid creating a larger privacy risk in the process of protecting children.

- **Data Fiduciary Accountability and Significant Data Fiduciaries**

The DPDP Act imposes general obligations upon Data Fiduciaries, including requirements concerning security safeguards and breach notification.[14] Organisations must implement appropriate technical and organisational measures to prevent personal data breaches. The statutory penalties can be substantial. The Schedule to the Act permits penalties extending to ₹250 crore for failure to implement reasonable security safeguards and up to ₹200 crore for specified breach-notification failures. The Act also creates the category of Significant Data Fiduciaries. Such entities may be subjected to additional obligations because their scale and nature of processing may create greater risks to individuals.[15] This risk-based approach is important because not all data processing creates identical risks. A small educational service processing limited information should not necessarily face the same compliance burden as a large platform processing data concerning millions of individuals. The challenge is to ensure that differentiated regulation does not become regulatory uncertainty. Clear criteria, transparent notification procedures and accessible guidance will be necessary.

- **Balancing Privacy and Technological Innovation**

➢ **Data as an Economic Resource**

Data has become a major driver of innovation. Artificial intelligence, machine learning, financial technology, healthcare analytics and personalised services depend heavily upon data. India's emerging digital economy requires access to data for research and development. Excessive regulatory burdens could disproportionately affect start-ups and small enterprises that lack sophisticated compliance departments. The DPDP framework attempts to address this concern through a relatively principles-based regulatory structure and differentiated obligations.

➢ **Privacy by Design**

Innovation and privacy should not be viewed as inherently contradictory. The appropriate objective is.[16] Privacy by design requires organisations to incorporate privacy safeguards at the

[14] Digital Personal Data Protection Act 2023, s 8.
[15] Digital Personal Data Protection Act 2023, s 10.
[16] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

ISSN: 2582-6433

technological development stage rather than attempting to address privacy concerns after a system has been deployed. For example, anonymisation, pseudonymisation, encryption, access controls, limited retention periods and privacy-preserving analytics can enable organisations to derive value from data without unnecessarily exposing individuals. The DPDP framework should therefore encourage technological solutions that reduce the amount of personal data collected and retained.

- **Artificial Intelligence**

Artificial intelligence presents a particularly difficult challenge. AI systems often require large datasets for training and optimisation. At the same time, AI can reproduce or amplify biases contained in datasets.[17] Data protection regulation therefore intersects with equality, non-discrimination and due process. Future Indian jurisprudence will need to address questions such as whether individuals should be informed when significant decisions concerning them are substantially influenced by automated systems, how algorithmic profiling should be regulated and what remedies should be available where automated processing produces discriminatory outcomes.

- **Cross-Border Data Transfers**

Digital commerce is inherently international. Indian organisations frequently rely upon cloud infrastructure and service providers located outside India.[18] The DPDP Act adopts a flexible approach to cross-border transfers. Rather than imposing an absolute localisation requirement, it permits transfers subject to restrictions that may be specified by the Central Government. This approach has advantages for innovation because excessive localisation can increase infrastructure costs and restrict access to global digital services. At the same time, unrestricted international transfers can create jurisdictional and enforcement difficulties. Data transferred outside India may become subject to foreign laws and governmental access regimes. The challenge is therefore to establish mechanisms that protect Indian Data Principals while maintaining international interoperability. India should consider adopting transparent criteria for determining jurisdictions where data transfers may be restricted and should promote international cooperation concerning data protection and law-enforcement access.

[17] Internet and Mobile Association of India v Reserve Bank of India (2020) 10 SCC 274 (proportionality in regulation affecting emerging digital technologies).
[18] Digital Personal Data Protection Act 2023, s 16.

ISSN: 2582-6433

- **State Interests and Governmental Access to Personal Data**

➢ **The State as a Data Processor**

The State is among the largest processors of personal information. Government agencies process data concerning identity, taxation, welfare benefits, healthcare, education, policing and public administration.[19] Data can improve service delivery and assist in preventing fraud and crime. However, concentration of personal information within governmental databases also creates significant surveillance risks. The constitutional question is therefore whether State processing remains within the boundaries of legality, necessity and proportionality.

➢ **Exemptions and Constitutional Safeguards**

One of the most debated aspects of the DPDP framework concerns exemptions and powers available to the State. The State may have legitimate reasons to process personal data without conventional consent—for example, providing public services, complying with legal obligations, responding to emergencies or protecting national security. However, broad exemptions can undermine the central objective of data protection if they are not accompanied by independent safeguards. The Supreme Court's privacy jurisprudence requires State interference with privacy to satisfy constitutional standards. Therefore, statutory exemptions should not be interpreted as eliminating constitutional review. The principles of legality, legitimate State aim, necessity and proportionality should remain applicable to State processing.

➢ **Surveillance and Informational Power**

Modern surveillance differs from traditional physical surveillance because digital systems permit the collection, aggregation and analysis of enormous amounts of information.[20] The aggregation of individually innocuous information can create highly detailed profiles. Consequently, the privacy risk does not arise only from the collection of sensitive information but also from the ability to combine different datasets. Independent oversight, audit mechanisms, purpose limitation and judicial remedies are therefore essential.

- **Institutional Framework: Data Protection Board of India**

The DPDP Act establishes the Data Protection Board of India as the principal regulatory and

[19] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[20] People's Union for Civil Liberties v Union of India (1997) 1 SCC 301 (telephone interception and procedural safeguards).

ISSN: 2582-6433

adjudicatory institution. The Rules provide for its functioning as a digital office and establish provisions concerning its composition and functioning.[21] The Board represents an important institutional development because effective data protection requires more than statutory rights. Individuals need a mechanism through which those rights can be enforced. Institutional independence is therefore critical. The regulator must be capable of exercising its functions impartially, including where violations involve powerful private entities or governmental bodies. The Board should consequently operate with transparent procedures, reasoned decisions, accessible complaint mechanisms and appropriate safeguards against institutional influence.

- ## Comparative Perspective: India and the European Union

The GDPR remains an important international reference point for data protection law. It establishes principles including lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.[22] The Indian framework shares several conceptual similarities with the GDPR, particularly regarding accountability, purpose limitation and individual rights. However, the DPDP Act adopts a more streamlined model and provides broader legislative space for governmental processing. The difference reflects different constitutional and institutional contexts. India must develop a regulatory model suited to its digital economy, administrative structure and constitutional framework rather than mechanically reproducing European legislation. Nevertheless, comparative experience demonstrates that effective data protection depends upon three elements: strong substantive rights, independent institutional enforcement and meaningful remedies.

- ## Major Challenges in the Indian Framework

  - ### Awareness and Digital Literacy

Limited digital literacy prevents many individuals from understanding how their personal data is collected, processed and shared. Consequently, consent may become merely formal rather than informed. Government, educational institutions and technology companies should promote privacy awareness through accessible digital-literacy programmes, regional-language information, simplified privacy notices and effective public awareness campaigns.[23]

[21] Digital Personal Data Protection Act 2023, ss 18–27.
[22] Regulation (EU) 2016/679 (General Data Protection Regulation), art 5.
[23] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1 (privacy, autonomy and informational control).

ISSN: 2582-6433

- **Regulatory Capacity**

Effective implementation of the DPDP framework requires a technically competent and adequately resourced Data Protection Board. Expertise in law, cybersecurity, artificial intelligence and digital forensics is essential. Transparent procedures, continuous training, sufficient financial resources and institutional independence will enable the Board to investigate violations effectively and provide timely regulatory guidance.[24]

- **State Exemptions**

Governmental exemptions may be necessary for national security, law enforcement and public administration, but unrestricted exemptions can threaten constitutional privacy. State processing should remain subject to legality, necessity and proportionality. Clear purpose limitations, access controls, retention periods, independent oversight and judicial review are necessary to prevent excessive governmental data processing.[25]

- **Enforcement against Global Technology Companies**

Global technology companies frequently operate across multiple jurisdictions, creating significant enforcement difficulties. Effective regulation requires international cooperation, information sharing and mechanisms for cross-border enforcement. India should strengthen cooperation with foreign regulators while establishing clear obligations for multinational enterprises processing Indian citizens' personal data and ensuring proportionate regulatory enforcement.[26]

- **Data Breaches and Cybersecurity**

Data breaches can cause financial loss, identity theft, reputational damage and serious privacy violations. Data Fiduciaries should therefore implement encryption, access controls, authentication, security audits and incident-response mechanisms. Timely breach notification and effective remedies are essential. Financial penalties should be supplemented by preventive compliance, cybersecurity assessments and organisational accountability.[27]

[24] Digital Personal Data Protection Act 2023, ss 18–27; Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[25] K.S. Puttaswamy (Retd) v Union of India (2019) 1 SCC 1; People's Union for Civil Liberties v Union of India (1997) 1 SCC 301.
[26] Shreya Singhal v Union of India (2015) 5 SCC 1; Anuradha Bhasin v Union of India (2020) 3 SCC 637.
[27] Digital Personal Data Protection Act 2023, s 8 and Schedule; Information Technology Act 2000, s 43A.

ISSN: 2582-6433

- **Recommendations**

The Digital Personal Data Protection framework represents an important development in Indian data governance; however, its effectiveness will ultimately depend upon implementation, institutional capacity and the protection of constitutional values. The following measures are recommended to achieve an appropriate balance between privacy, innovation and legitimate State interests.

➢ **Constitutional Proportionality in State Data Processing**

All significant processing of personal data by government authorities should be governed by the principles of legality, necessity, legitimate State objective and proportionality. The existence of statutory authority should not, by itself, justify unrestricted collection or processing of personal information. Government agencies should demonstrate that the data sought is necessary for a legitimate public purpose and that less intrusive alternatives are unavailable. Judicial review should remain available where State action substantially interferes with privacy and informational autonomy.[28]

➢ **Strengthening the Independence of the Data Protection Board**

The effectiveness of any data protection regime depends upon the independence and capacity of its regulatory institution. The Data Protection Board of India should possess adequate financial, technical and administrative resources and should function through transparent and accountable procedures. Its members should have expertise in law, technology, cybersecurity and data governance. Institutional safeguards should ensure that regulatory decisions are not improperly influenced by either government authorities or powerful private entities.[29]

➢ **Meaningful and Informed Consent**

Consent should represent a genuine exercise of individual choice rather than a formal acceptance of lengthy terms and conditions. Data Fiduciaries should provide concise, accessible and intelligible notices explaining what information is collected, why it is collected and how it will be used. Consent interfaces should avoid manipulative design, pre-selected options and unnecessary barriers to withdrawal. Particular attention should be given to individuals with limited digital literacy.[30]

[28] K.S. Puttaswamy (Retd) v Union of India (2019) 1 SCC 1.
[29] Digital Personal Data Protection Act 2023, ss 18–27.
[30] Digital Personal Data Protection Act 2023, s 6; Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.

ISSN: 2582-6433

- **Promoting Privacy-by-Design**

Privacy protection should be incorporated into digital products and services from the earliest stage of technological development. Organisations should adopt measures such as encryption, pseudonymisation, anonymisation, access controls and privacy-preserving analytics. Privacy-by-design can enable innovation without requiring unrestricted access to identifiable personal information. Regulatory guidance and industry standards should encourage businesses, particularly start-ups, to integrate privacy safeguards into technological design.[31]

- **Data Minimisation and Retention Controls**

Organisations should collect only the personal data that is necessary and proportionate to a specified purpose. Unnecessary accumulation of personal information increases the consequences of data breaches and facilitates secondary uses beyond the original purpose. Data Fiduciaries should establish documented retention schedules and securely delete or anonymise information once the legitimate purpose for processing has expired.[32]

- **Enhanced Protection for Children and Vulnerable Individuals**

Children require heightened protection because they may not fully appreciate the long-term consequences of digital disclosure. Strong safeguards should regulate profiling, behavioural monitoring and targeted commercial practices involving children. However, verification mechanisms should themselves be privacy-preserving and should not require excessive collection of identity information. Similar risk-sensitive safeguards should be considered for other vulnerable groups.[33]

- **Transparent Cross-Border Data Transfers**

India's digital economy depends substantially upon international cloud computing, technology services and cross-border commerce. Cross-border transfers should therefore not be prohibited unnecessarily. At the same time, Data Principals should receive reasonable protection when their information is transferred to foreign jurisdictions. India should adopt transparent criteria for assessing destination jurisdictions and encourage contractual, technical and institutional safeguards for international transfers.

[31] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[32] Regulation (EU) 2016/679, art 5(1)(c) (data minimisation), as a comparative principle.
[33] Digital Personal Data Protection Act 2023, s 9.

ISSN: 2582-6433

- **Accessible Grievance Redressal**

Data protection rights are meaningful only when individuals can enforce them effectively. Grievance mechanisms should therefore be simple, inexpensive, time-bound and digitally accessible, while also accommodating individuals with limited digital literacy. The regulatory framework should provide clear escalation mechanisms where Data Fiduciaries fail to resolve complaints. Remedies should include appropriate correction, deletion, restoration of rights and compensation or penalties where legally justified.[34]

- **Independent Auditing of Government Databases**

Government databases containing sensitive personal information should be subject to periodic independent privacy and cybersecurity audits. Authorities should maintain clear access-control systems, activity logs, retention schedules and procedures for detecting unauthorised access. Independent audits can reduce the risks associated with excessive data accumulation, internal misuse and cybersecurity vulnerabilities while improving public confidence in digital governance.[35]

- **International Cooperation and Harmonisation**

Personal data frequently crosses national borders, while cyberattacks and data breaches increasingly have transnational dimensions. India should strengthen cooperation with foreign regulators and international organisations concerning cross-border enforcement, cybersecurity, data breach investigations and lawful governmental access to information. Greater compatibility with international data protection principles would also facilitate international trade and technological cooperation while strengthening protection for Indian Data Principals.[36]

• Conclusion

The Digital Personal Data Protection Act 2023 represents a significant transformation of India's legal approach to personal data. It establishes statutory recognition of individual rights while attempting to facilitate lawful data processing and technological development. The Digital Personal Data Protection Rules 2025 further provide the operational architecture necessary for

[34] Digital Personal Data Protection Act 2023, ss 11–15.
[35] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1; People's Union for Civil Liberties v Union of India (1997) 1 SCC 301.
[36] Digital Personal Data Protection Act 2023, s 16; Regulation (EU) 2016/679, arts 44–49.

ISSN: 2582-6433

implementation. The Government has adopted a phased commencement model, with the substantive provisions scheduled to become operational after the prescribed transition period.[37] The principal challenge is not simply the protection of privacy against private corporations. It is the creation of a constitutional data governance framework capable of regulating both private and public power.[38] Data has enormous social and economic value. It can improve healthcare, strengthen public administration, facilitate financial inclusion and accelerate artificial intelligence and digital innovation. Yet unrestricted collection and processing can undermine autonomy, dignity and democratic freedom. India should therefore reject the false choice between privacy and innovation. Strong privacy protection can itself create trust, and trust is essential for sustainable digital innovation. The appropriate objective is a system in which data may be processed for legitimate purposes while individuals retain meaningful protection against misuse. The State, similarly, must be able to process information for legitimate public purposes, but such powers should remain subject to legality, necessity, proportionality, transparency and institutional accountability.[39] The future of Indian data protection law will ultimately depend less upon the text of the legislation alone and more upon its interpretation and implementation. Courts, regulators, businesses and government agencies must collectively ensure that digital transformation does not become a justification for excessive informational control. The constitutional promise of privacy requires a legal order in which technological progress and individual dignity reinforce rather than undermine each other.[40] The DPDP framework therefore marks the beginning, rather than the end, of India's data protection journey. Its long-term legitimacy will depend upon whether it succeeds in creating an environment in which privacy is protected, innovation is encouraged and State power remains constitutionally accountable.

[37] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1; Digital Personal Data Protection Act 2023.
[38] K.S. Puttaswamy (Retd) v Union of India (2019) 1 SCC 1.
[39] K.S. Puttaswamy (Retd) v Union of India (2019) 1 SCC 1; People's Union for Civil Liberties v Union of India (1997) 1 SCC 301.
[40] Anuradha Bhasin v Union of India (2020) 3 SCC 637; Shreya Singhal v Union of India (2015) 5 SCC 1.