INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

A CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT (DPDPA) 2023 IN INDIA

AUTHORED BY - E YESHVANT NEMALAN & B RAJU LAKSHMANAN
(2nd Year B.Com,LLB(hons.)).
Affiliation: Sastra University Thanjavur

ABSTRACT

"Privacy Rights Data Protection Governance"

This research paper examines the Digital Personal Data Protection Act, 2023 and its significance in establishing a comprehensive legal framework for data privacy and protection in India. The study analyses the evolution of privacy jurisprudence from the Information Technology Act, 2000 to the landmark judgment in Justice K.S. Puttaswamy v. Union of India, which recognised privacy as a fundamental right under Article 21 of the Constitution. The paper critically evaluates the major provisions of the DPDPA, including consent-based processing, obligations of data fiduciaries, rights of data principals, regulation of children's data, and the functioning of the Data Protection Board of India. It further explores concerns regarding government exemptions, institutional independence, surveillance implications, and lack of compensation mechanisms for affected individuals. Comparative references to the European Union's GDPR are used to assess the adequacy of the Indian framework in a global context. The paper concludes that while the DPDPA marks a major legislative development in Indian privacy law, its practical effectiveness will depend upon transparent implementation, strong regulatory safeguards, and judicial oversight.

INTRODUCTION

India's economic transformation over the past three decades has been nothing short of remarkable. From a largely agrarian and manufacturing-driven economy, the country has emerged as one of the world's foremost digital powerhouses. With over 850 million active internet users, a thriving fintech ecosystem, and a government committed to the ambitious 'Digital India' initiative, personal data has become the most valuable commodity of the twenty-first century. Every digital transaction — from a UPI payment to a ride-hailing request —

ISSN: 2582-6433

generates data points that are collected, processed, monetised, and shared by a complex web of private corporations and state agencies. For decades, this immense flow of personal information operated in a near-total legal vacuum, governed only by the skeletal and largely inadequate provisions of the Information Technology Act, 2000.

The inflection point arrived on 24 August 2017, when a nine-judge Constitution Bench of the Supreme Court of India delivered its landmark verdict in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[1] Unanimously, the Court held that the right to privacy is a fundamental right, intrinsic to life and liberty and guaranteed under Article 21 of the Constitution of India. The judgment did not merely recognise privacy as a value — it constitutionalised it, asserting that informational privacy — the right to control one's personal data — forms an essential component of this fundamental guarantee. The ruling sent an unequivocal signal to the legislature: a comprehensive data protection framework was no longer a policy aspiration but a constitutional imperative.

Six years of parliamentary deliberation, multiple drafts, sustained civil society advocacy, and intense lobbying by the technology industry culminated in the passage of the Digital Personal Data Protection Act, 2023 (hereinafter 'the Act' or 'DPDPA 2023').[2] Enacted in August 2023, the legislation represents India's first dedicated, comprehensive law for the protection of digital personal data. It introduces a rights-based framework for individuals, places obligations on entities processing data, and establishes an adjudicatory body to enforce its provisions.

Yet the Act is as notable for what it does not do as for what it does. Its lean, principles-based drafting leaves much to subordinate rule-making. Its wide exemptions for the state raise serious concerns about surveillance overreach. Its adjudicatory body lacks the structural independence necessary for robust enforcement. This paper undertakes a critical evaluation of whether the DPDPA 2023 adequately balances the individual's fundamental right to privacy against the twin imperatives of state security and economic innovation. It argues that while the Act is a historic milestone in India's legal evolution, its ultimate efficacy will be determined not by the statute itself, but by the Rules yet to be notified and the political will to enforce them honestly.

[1] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[2] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

ISSN: 2582-6433

HISTORICAL BACKGROUND AND THE LEGAL VACUUM

Before the DPDPA 2023, the primary legislative instrument governing data in India was the Information Technology Act, 2000 (hereinafter 'the IT Act').[3] Enacted primarily to facilitate e-commerce and penalise cybercrime, the IT Act was never designed as a comprehensive privacy statute. Its approach to data protection was narrow, reactive, and manifestly insufficient for the data-intensive economy that India was rapidly becoming.

Section 43A of the IT Act, inserted by amendment in 2008, imposed a civil liability on 'body corporates' that handled 'sensitive personal data or information' (SPDI) negligently, causing wrongful loss or gain. The Sensitive Personal Data or Information Rules of 2011, framed under Section 43A, constituted India's closest approximation to data protection regulation before 2023. These Rules defined categories of sensitive data — including passwords, financial information, health records, and biometric data — and imposed rudimentary obligations of consent and disclosure.[4]

However, the SPDI Rules suffered from crippling limitations. They applied only to 'body corporates' and thus excluded state agencies, the single largest collector of personal data in India. The Rules conflated the concepts of consent and contractual performance, providing that consent was 'deemed' to have been given when data was provided for the performance of a lawful contract — a provision so broad as to render the consent requirement largely meaningless. The Rules also lacked a dedicated enforcement mechanism, leaving aggrieved individuals to pursue remedies through the civil courts — a process that was expensive, time-consuming, and largely inaccessible to ordinary citizens. Furthermore, the categorisation of 'sensitive' data was static and failed to account for the evolving nature of digital privacy harms, particularly the privacy risks arising from the aggregation of seemingly innocuous, non-sensitive data points.

The IT Act and its attendant Rules were, in effect, a framework designed for a pre-smartphone, pre-social media, pre-big data world. As India's digital economy exploded, the regulatory apparatus remained frozen in 2011.

[3] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[4] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

ISSN: 2582-6433

The Puttaswamy judgment of 2017 catalysed legislative action. The Supreme Court, while declaring privacy a fundamental right, expressly noted the absence of a data protection law and implicitly called upon Parliament to remedy the lacuna. In response, the Ministry of Electronics and Information Technology (MeitY) constituted a Committee of Experts on Data Protection chaired by retired Justice B.N. Srikrishna.

The Srikrishna Committee submitted its report and a draft Personal Data Protection Bill in July 2018. The report was a sophisticated document that drew upon global best practices, particularly the European Union's General Data Protection Regulation (GDPR), while attempting to calibrate obligations to the Indian context. It proposed a tiered framework for personal and sensitive personal data, an independent Data Protection Authority, data localisation requirements, and a right to data portability.

The government introduced the Personal Data Protection Bill, 2019 in Parliament. The Bill was referred to a Joint Parliamentary Committee (JPC), which deliberated for over two years and submitted a comprehensive report in December 2021. However, in an unexpected development, the government withdrew the 2019 Bill entirely in August 2022, citing the need to replace it with a 'comprehensive legal framework.' The withdrawal attracted significant criticism, as it consigned years of legislative and expert effort to the archives. A simpler, leaner draft — which would ultimately become the DPDPA 2023 — was then circulated for public consultation before being introduced and passed in both Houses of Parliament with remarkable legislative speed in August 2023.

The shift from the 2019 Bill's dense, prescriptive architecture to the 2023 Act's lean, principles-based approach was deliberate and significant. Critics noted that several robust protections from the Srikrishna report — including the concept of a truly independent data protection authority and strict data localisation requirements — were substantially diluted or abandoned.

KEY PROVISIONS OF THE DPDPA 2023

The DPDPA 2023 applies to the processing of 'digital personal data' — that is, data about an individual that is capable of identifying that individual, and which exists in digital form or has been digitised. Notably, the Act excludes personal data processed for purely personal or domestic purposes, as well as data made publicly available by the data principal themselves or under any law for the time being in force. The exclusion of non-digital personal data represents

ISSN: 2582-6433

a significant gap, as vast quantities of personal information — particularly in rural India — still exist in physical form and may be digitised without adequate safeguards.

In a significant assertion of extra-territorial jurisdiction, Section 3(b) of the Act extends its application to the processing of personal data outside India where such processing is 'in connection with any activity related to offering of goods or services to Data Principals within the territory of India.' This mirrors the GDPR's extra-territorial reach and signals India's intent to regulate global technology corporations that target Indian consumers, regardless of where those corporations are incorporated or where data is actually processed.

The Act introduces two central actors in the data processing relationship. The 'Data Principal' is the individual to whom the personal data relates — in effect, the data subject. The 'Data Fiduciary' is the person (including a legal entity) who determines the purpose and means of processing personal data — equivalent to the 'data controller' under the GDPR. The choice of the term 'fiduciary' is deliberate and conceptually significant: it imports into the data processing relationship a duty of trust, implying that the entity processing data must act in the interest of the individual whose data it holds, not merely in its own commercial interest.

The Act imposes an extensive range of obligations on Data Fiduciaries. These include the duty to maintain the accuracy and completeness of personal data, to implement reasonable security safeguards to prevent data breaches, to notify the Data Protection Board and affected Data Principals in the event of a breach, and to erase data once the purpose for which it was collected has been fulfilled or upon withdrawal of consent. The Act also provides for the designation of 'Significant Data Fiduciaries' — entities whose processing of data, by virtue of its volume, sensitivity, or potential for harm, warrants heightened obligations, including the appointment of a Data Protection Officer and the conduct of periodic Data Protection Impact Assessments. Corresponding to the obligations of fiduciaries are the rights of Data Principals. Section 11 grants the right to access information about the personal data held by a fiduciary. Section 12 provides the right to correction and erasure of inaccurate, incomplete, or outdated data. Section 13 provides the right of grievance redressal, requiring fiduciaries to establish accessible mechanisms for the resolution of complaints. Section 14 grants the right to nominate another individual to exercise data rights in the event of death or incapacity — a uniquely Indian addition that recognises the importance of digital assets in succession.

ISSN: 2582-6433

A notable and controversial omission is the absence of a right to data portability — the right to receive one's own data in a machine-readable format and transfer it to another provider. The Srikrishna Committee had recommended portability as a mechanism to promote competition and reduce lock-in to dominant platforms. Its exclusion from the final statute has been criticised as a capitulation to the interests of large data-rich corporations.

Consent is the foundational basis for data processing under the DPDPA 2023. Section 6 requires that processing of personal data be preceded by the provision of a 'Notice' to the Data Principal, describing in clear and plain language the personal data to be collected and the purpose for which it will be processed. Consent must be given through a 'clear affirmative action' — the Act expressly prohibiting implied consent through inaction, pre-ticked boxes, or bundled terms of service. This represents a significant improvement over the nebulous consent standards of the SPDI Rules.

The Act also introduces the innovative concept of a 'Consent Manager' — a platform registered with and regulated by the Data Protection Board through which Data Principals may give, manage, review, and withdraw consent across multiple fiduciaries. This intermediary mechanism is a distinctive Indian innovation, designed to address the practical challenge of consent fragmentation across hundreds of digital services. A citizen might use dozens of applications that process personal data; the Consent Manager is envisaged as a single dashboard through which she can exercise control over all of them. The detailed architecture and operational requirements of Consent Managers will be specified in the Rules, and their effectiveness will depend entirely on whether those Rules mandate genuine functionality or permit superficial compliance.

Crucially, consent is not required for what the Act terms 'Legitimate Uses' — specified categories of processing that are deemed lawful without individual consent. These include the performance of a function of the state for the provision of a service or benefit to the Data Principal; compliance with a court judgment or order; response to a medical emergency threatening life; and the purposes of employment. The breadth of the 'state function' exception is particularly significant: in a country where the government is the largest provider of welfare services, the exemption from consent for state processing covers an enormous volume of citizen data.

ISSN: 2582-6433

Section 9 of the Act imposes stringent requirements on the processing of children's data, defined as individuals below the age of eighteen years. Fiduciaries processing children's data must obtain 'verifiable parental consent' — a technically demanding requirement given the difficulty of age and identity verification in digital environments. The Act further prohibits Data Fiduciaries from processing children's data in a manner that is detrimental to their well-being, and expressly bans tracking and behavioural monitoring of children, as well as targeted advertising directed at minors. These provisions represent some of the most robust protections in the Act, reflecting global concerns about the exploitation of minors in the digital ecosystem. The government retains the power to exempt certain classes of fiduciaries from the parental consent requirement, subject to conditions — a necessary flexibility for educational institutions and child welfare services.

The Data Protection Board of India (DPB), established under Chapter VI of the Act, is the designated adjudicatory body responsible for inquiring into complaints, determining violations, and levying financial penalties. The Act imposes substantial penalties: up to Rs. 250 crore (approximately USD 30 million) for a failure to implement reasonable security safeguards leading to a data breach, and up to Rs. 200 crore for failure to notify the Board of a breach. The total quantum of penalties that can be levied under the Act may reach Rs. 250 crore for any single violation, which represents a meaningful deterrent for larger corporations.

However — and this is a point of profound significance — the Act provides no mechanism for the payment of compensation to the Data Principal, the individual who has suffered harm as a consequence of the data breach or privacy violation. Penalties flow to the Consolidated Fund of India; the victim receives nothing. This contrasts sharply with the GDPR, under which data subjects have an express right to compensation for material and non-material damage. The absence of a victim compensation mechanism fundamentally undermines the Act's rights-based character.

CRITICAL CHALLENGES AND CONTROVERSIES

The most trenchant criticism levelled at the DPDPA 2023 concerns the breadth of exemptions available to the Central Government and its agencies. Section 18 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 interest of 'sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or preventing

ISSN: 2582-6433

incitement to any cognisable offence.' The grounds for exemption are identical to those enumerated in Article 19(2) of the Constitution, which permits reasonable restrictions on freedom of speech — but the exemption mechanism of the DPDPA is notably broader: it operates not as a judicially reviewable restriction but as an executive notification that may be issued without legislative oversight or independent scrutiny.

The implications of this provision are staggering. The government may, by a simple executive notification, exempt the Intelligence Bureau, the Research and Analysis Wing, or any other state agency from the obligation to obtain consent, the obligation to maintain data accuracy, the obligation to erase data, and every other protection that the Act confers on citizens. This is not a narrowly tailored national security exception — it is a structural carve-out that, if used expansively, could render the Act's protections illusory for the very contexts in which privacy is most at risk: mass surveillance by the state.

The Supreme Court in *Puttaswamy* held that any limitation on the right to privacy must satisfy the triple test of legality, necessity, and proportionality. It is doubtful that a blanket executive exemption, unaccompanied by judicial oversight or parliamentary accountability, can withstand this constitutional scrutiny. Digital rights advocates, including the Internet Freedom Foundation, have argued that Section 18 effectively creates a second tier of citizens — those whose data is processed by private entities and who enjoy the Act's protections, and those whose data is processed by the state and who may enjoy no protections at all.

The structural independence of a data protection authority is universally regarded as the cornerstone of effective privacy enforcement. An authority beholden to the executive for its appointments, budget, and continuance cannot credibly regulate the government's own data processing activities. The GDPR mandates that supervisory authorities act 'with complete independence,' and this requirement is treated as a constitutional imperative in the European context.

The DPDPA 2023 falls substantially short of this standard. The members of the Data Protection Board are appointed by the Central Government on the recommendation of a selection committee whose composition is prescribed by Rules that have not yet been notified. The government also determines the terms and conditions of service of Board members, including their salaries, allowances, and removal procedures. There is no provision requiring

ISSN: 2582-6433

parliamentary confirmation of appointments, no prohibition on the re-appointment of members (which creates incentives for accommodating the appointing authority), and no guaranteed minimum budget.

This institutional design mirrors the criticism that has been made of other sector regulators: their formal independence is undercut by their practical dependence on the executive for personnel and resources. A Data Protection Board that is materially dependent on the government is ill-equipped to adjudicate complaints against government agencies — a fundamental conflict of interest that the Act does nothing to resolve.

The Act's provisions on erasure — the 'right to be forgotten' in European parlance — create a significant tension with India's Right to Information Act, 2005 (RTI Act), a statute of enormous importance to accountability and democratic governance. The RTI Act establishes the public's right to access information held by public authorities, including personal information in certain circumstances. It has been used by journalists, activists, and ordinary citizens to expose corruption, demand accountability, and vindicate the right to know.

When a Data Principal exercises the right to erasure under the DPDPA 2023, and the data sought to be erased is information held by a public authority that may also be subject to RTI disclosure, the two statutes come into direct conflict. The DPDPA 2023 does not explicitly address this conflict, creating a zone of legal uncertainty. Critics fear that data erasure requests could be weaponised by powerful individuals — including public officials — to remove information from the public domain that should rightly remain accessible. The absence of a clear hierarchy between the two statutes is a significant legislative oversight that will inevitably generate litigation.

COMPARATIVE ANALYSIS

A comparison with the European Union's General Data Protection Regulation illuminates the philosophical divergence between India's approach and the global standard-setter in data protection law. The GDPR, which came into force in May 2018, is a comprehensive, prescriptive instrument that specifies in considerable detail the conditions under which personal data may be processed, the rights of data subjects, the obligations of controllers and processors, and the powers of supervisory authorities. It has been described as the world's most influential data protection law, inspiring similar legislation in over 130 countries.

ISSN: 2582-6433

The DPDPA 2023, by contrast, is lean, principles-based, and heavily reliant on subordinate legislation. Where the GDPR specifies six lawful bases for processing data, the DPDPA 2023 operates on a binary of consent and legitimate uses. Where the GDPR provides for a right to data portability, the DPDPA 2023 does not. Where the GDPR mandates detailed records of processing activities, the DPDPA 2023 leaves such requirements to the Rules. Where the GDPR grants supervisory authorities guaranteed budgetary independence, the DPDPA 2023 makes the Board financially dependent on the Central Government.

Proponents of the DPDPA's lean approach argue that over-prescription leads to compliance theatre — organisations investing in documentation rather than genuine data protection — and that a principles-based framework affords greater flexibility as technology evolves. There is merit in this position: the GDPR has indeed generated enormous compliance costs, particularly for small and medium enterprises. However, the counter-argument is that without prescription, there is no accountability; principles without rules are aspirations, not obligations. The DPDPA 2023's effectiveness will depend critically on whether the Rules, when notified, provide the specificity that the statute itself lacks.

A further point of comparison is the treatment of data subject rights. The GDPR's Article 82 provides an explicit right to compensation for material and non-material damage arising from GDPR violations. The DPDPA 2023's omission of a victim compensation mechanism is, from a comparative perspective, a significant regression — particularly for a statute enacted six years after the GDPR came into force and with the benefit of that experience.

The question of where data may be stored and processed is of immense commercial and geopolitical significance. The 2019 Bill proposed strict data localisation — requiring certain categories of sensitive and critical personal data to be stored exclusively in India. This provision was strongly opposed by global technology companies and, notably, by the United States government, which viewed it as a barrier to trade.

The DPDPA 2023 takes a markedly different approach. Section 16 empowers the Central Government to restrict the transfer of personal data to specified countries or territories, but the default is permissive — personal data may be transferred across borders to any country not explicitly restricted. This represents a significant liberalisation from the 2019 Bill's position and aligns India more closely with the GDPR's adequacy-based framework, though without

ISSN: 2582-6433

the GDPR's elaborate mechanisms for assessing the adequacy of protection in recipient countries. The list of restricted countries has not yet been published, and the criteria for restriction remain opaque. The liberalised approach has been welcomed by industry but criticised by data sovereignty advocates who argue that unrestricted cross-border data flows expose Indian citizens' data to jurisdictions with weaker privacy protections.

CONCLUSION AND RECOMMENDATIONS

The Digital Personal Data Protection Act, 2023 is a landmark enactment in India's legal history. For the first time, India has a dedicated, comprehensive statute that recognises the individual as a 'Data Principal' — not merely a data subject — and places corresponding obligations of trust on those who collect and process her information. The Act implements the constitutional mandate of the Puttaswamy judgment, translating the fundamental right to privacy into actionable legal rights and enforceable duties. It introduces the innovative Consent Manager mechanism, imposes significant financial penalties for data breaches, and extends India's jurisdictional reach to foreign entities targeting Indian consumers.

And yet, for all its historic significance, the Act is more a framework than a finished edifice. Its skeleton is present, but the flesh — the Rules, the notifications, the guidelines — has yet to be attached. The experience of the SPDI Rules demonstrates that subordinate legislation can be either the salvation or the undoing of a data protection statute. If the Rules under the DPDPA 2023 are drafted with the interests of citizens at their centre — providing detailed and enforceable guidance on consent mechanisms, security standards, data breach notification timelines, and the scope of government exemptions — the Act has the potential to become a genuinely transformative instrument. If, as many fear, the Rules are drafted to minimise regulatory burden on industry and maximise government discretion, the Act's protections will remain largely illusory.

Based on the foregoing analysis, this paper advances the following recommendations for strengthening India's data protection framework:

First, the independence of the Data Protection Board must be structurally guaranteed. Appointments to the Board should be made through a transparent, multi-stakeholder process involving parliamentary oversight, with fixed, non-renewable terms and security of tenure that insulates members from executive pressure. The Board's budget should be secured through statutory formula rather than annual governmental allocation.

ISSN: 2582-6433

Second, the scope of government exemptions under Section 18 must be narrowed and judicially supervised. The provision as currently drafted is constitutionally suspect in light of the proportionality requirement articulated in *Puttaswamy*. The Rules should specify the categories of state processing that are exempt, the duration of permissible exemptions, and the mandatory oversight mechanisms — including judicial authorisation — that must attend any exemption from core privacy protections.

Third, a victim compensation mechanism must be introduced, either through the Rules or by statutory amendment. The current framework, in which all penalties flow to the state while victims receive nothing, is inconsistent with the rights-based character of the legislation and the compensatory principle articulated in the Supreme Court's privacy jurisprudence.

Fourth, the right to data portability should be incorporated into the Act or mandated through Rules applicable to Significant Data Fiduciaries. Portability is essential for competitive markets in data-intensive sectors such as financial services and healthcare, and its absence entrenches the market power of dominant platforms.

Fifth, the relationship between the DPDPA 2023 and the Right to Information Act, 2005 must be clarified through explicit statutory or regulatory provision. A framework that protects genuine privacy interests while preserving the public's right to accountability information is essential for both the integrity of data protection and the health of Indian democracy.

The DPDPA 2023 represents the beginning, not the end, of India's journey toward a mature data protection ecosystem. The *Puttaswamy* Court declared that privacy is not a gift from the state but an inalienable attribute of human dignity. The true measure of this statute will be whether, in the years to come, it upholds that declaration in practice — not merely in preamble.

BIBLIOGRAPHY

- Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India)
- Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India).
- Right to Information Act, 2005, No. 22, Acts of Parliament, 2005
- General Data Protection Regulation (EU) 2016/679, 2016
- Arghya Sengupta & Aparajita Lath, 'Privacy After Puttaswamy: Themes, Processes and Trajectories'
- Usha Ramanathan, 'A Unique Identity Bill' 48(2) *Economic and Political Weekly* 10

ISSN: 2582-6433

(2013).

- Internet Freedom Foundation, *Analysis of the Digital Personal Data Protection Act, 2023* (August 2023), available at https://internetfreedom.in.
- https://wikipedia.com