DBRANLU LAW REVIEW 2025

CONTENTS

Articles

TOWARDS PRIVACY-CENTRIC GOVERNANCE: ANALYZING INDIA'S DATA PROTECTION TRAJECTORY

- *Divya Singh[*] and Dr. Harish Tiwari[**]*

ABSTRACT

With the technological innovations gaining momentum, it is leading to the transformation of societies worldwide. Owing to these innovations, data is transcending the geographical boundaries thereby raising pressing concerns with regard to its effective regulation and safeguard. The collection, storage and utilization of vast amounts of data have become integral to numerous business and governmental operations. As a result, identity thefts, data breaches and the potential misuse of personal data have become pervasive threats. This rapid digitization and unprecedented growth in data generation, acquisition, and utilisation across public and private sector ecosystems has necessitated legal frameworks harmonising user rights with commercial interests globally. In the pursuit of strengthening data privacy, India has made notable progress by recently enacting the Digital Personal Data Protection Act 2023 modelled on the EU's pioneer GDPR standards. This study traces the genesis of the data protection legislation in the Indian subcontinent and delves into the inadequacies of the DPDP Act, 2023 in comprehensively addressing digital privacy concerns. Furthermore, the study proposes targeted measures that policymakers could consider to enhance data protection in the age of digital privacy.

Keywords: ***Data Protection, Right to Privacy, Srikrishna Committee, Digital Personal Data Protection Act 2023***

I. INTRODUCTION

In the modern digital age, the data protection and privacy right has grown into an increasingly vital issue. With rapid advancements in technology enabling more extensive data collection, analysis, and use, there have been increasing concerns regarding the potential for misuse and

[*] *5th Year Law Student, CHRIST (deemed to be University), Delhi NCR.*
[**] *Assistant Professor, CHRIST (deemed to be University), Delhi NCR.*

abuse of personal data.[1] This has led many countries to develop comprehensive legal frameworks regulating data protection.[2] In India, activism around data protection and privacy rights gained significant momentum after the 2017 Puttaswamy judgement of the Supreme Court, which ruled that the privacy right is a fundamental right under the Constitution of India.[3] This paved the path for India to enact its own data protection law. Following that, the Personal Data Protection Bill ("PDP Bill") was proposed in 2019[4], went through several amendments, and was finally enacted as the Digital Personal Data Protection Act ("DPDP Act") in 2023.

The DPDP Act controls how both the private organisations and the government process personal data by establishing a legal foundation for data protection in India.[5] Mandatory consent requirements for the collection and processing of personal data, limitations on cross-border data transfers, responsibilities for data fiduciaries and processors, data localisation standards, and sanctions for non-compliance are a few of its important characteristics. The law is still in the early stages of implementation and its complete impact remains to be seen.

Part II of this paper gives the historical context of the data protection legislation in India focussing on the pre-independence and post-independence data protection measures. It conducts an analysis of the IT Act 2000, IT Rules 2011, The Puttaswamy Judgement, The PDP Bill 2019, The DPDP Bill 2022 highlighting the lacunas in these laws resulting in their incapability to effectively regulate digital privacy and leading to the enactment of the DPDP Act 2023.

Part III of this paper critically analyses the DPDP Act, 2023 and brings forth its unique characteristics. Part IV of this paper highlights the inadequacies underlining the DPDP Act, 2023. Part V of this paper enumerates the policy recommendations to enhance the act's data security and privacy measures.

---

[1] *Graham Greenleaf, Data Protection in a Globalised Network, 10 UNSWLRS 221, 228 (2021).*

[2] *United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development, U.N. Doc. UNCTAD/DTL/STICT/2016/1 (Apr. 19, 2016).*

[3] *Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.*

[4] *The Personal Data Protection Bill 2019.*

[5] *The Digital Personal Data Protection Act, 2023, § 3, No. 22, Acts of Parliament, 2023 (India).*

II. HISTORICAL BACKDROP OF THE DATA PROTECTION LAW IN INDIA

India's narrative towards an effective and robust data protection legislation can be branched off into two phases. The first phase is the pre-independence phase which saw the glimpse of the rudimentary data protection measures while the second phase saw significant developments ranging from the Puttaswamy judgement to the introduction of the PDP Bill, 2019 and to the enactment of the DPDP Act, 2023.

2.1. Pre-Independence – Mid-20th Century

Data protection regulation in India has its roots in the pre-independence era, when the colonial government implemented limited policies and measures aimed at protecting certain types of private information. While comprehensive data protection legislation was still decades away, the early twentieth century saw Indian policymakers grapple with balancing privacy rights, government interests, and economic priorities even during colonial rule. One of the first examples was the Census Act of 1948, which guaranteed confidentiality to census data. The Act forbade the disclosure of any data collected during the census process that would identify a specific individual, though aggregate statistical data could be published.[6] This demonstrated an early recognition that personal information documented by the government deserved privacy protections.[7]

An important development came in the 1955 Report on the Revision of the Patent Law by Justice (Dr.) Bakshi Tek Chand which recommended limiting access to secret patent documents to only the "least number of persons in the Patent Office as may be necessary" to reduce potential leakage of sensitive commercial information. The report acknowledged the economic damage that could occur from disclosure of confidential documentation submitted by patent applicants. This reflected an understanding that certain types of private corporate or business information may warrant government restrictions on access. In 1958, the government implemented stringent controls specifically aimed at protecting individual privacy under the new Aircraft Rules.[8] The regulations placed limits on aerial photography to prevent infringement on the "right of the public to reasonable privacy." This was one of the earliest legislative attempts in India to codify privacy as an enumerated right deserving protection. Additional considerations for data privacy came about through case laws prior to independence,

[6] *The Census Act, 1948, § 15(1), No. 37, Acts of Parliament, 1948 (India).*
[7] *The Collection of Statistics Act, 2009, § 8(1), No. 7, Acts of Parliament, 2009 (India).*
[8] *The Aircraft Rules 1937.*

notably the landmark 1959 ruling in M.P. Sharma and Others v Satish Chandra.[9] Though the Supreme Court's verdict declined to recognise a generalised right to privacy under the Constitution of India, the judgement acknowledged that certain private matters may require safeguarding from governmental intrusion. This laid the bedrock for expanded privacy rights.

2.2. Post Independence – Present

India's legal framework has evolved significantly since gaining independence in 1947, shifting away from colonial laws towards a more progressive rights-based system aimed at social welfare and equitable justice. The journey of data protection regulation in India has traced an incremental path from limited sectoral safeguards to a comprehensive cross-sectoral framework that keeps pace with global best practices.

2.2.1. The IT Act 2000: India's first step towards data privacy regulation

The Information Technology (IT) Act 2000, the nation's first piece of legislation governing data practices, sowed the seed by introducing privacy protections for sensitive personal data.[10] However, the IT Act was primarily focused on facilitating e-commerce and e-governance, with data protection obligations introduced as a complementary afterthought. It contains basic data privacy protections, prohibiting unauthorised access, disclosure, and damage to electronic information. However, its applicability is limited, focusing chiefly on corporate data security practices rather than individual privacy rights.[11] Over time, the narrow scope and piecemeal privacy protections of the IT Act were deemed insufficient in the context of proliferation of data gathering and processing capabilities. The limitations stemmed from lack of definition around concepts such as ‘sensitive personal data’, absence of specifying purposes for data collection or explicit consent requirements, and lack of robust grievance redressal mechanisms.

Later on, the IT Rules, 2011 were notified under section 43A of the IT Act, 2000 in April 2011.[12] The goal was to mandate the usage of adequate security techniques and procedures

[9] *AIR 1954 SC 300.*
[10] *The Information Technology Act, 2000, § 43A, Acts of Parliament, 2000 (India).*
[11] *Rahul Matthan, Takshashila Discussion Document- Beyond Consent: A New Paradigm for Data Protection, TAKSHASHILA INSTITUTION (July 19, 2017), https://takshashila.org.in/research/discussion-document-beyond-consent-new-paradigm-data-protection.*

[12] *Information Technology Rules 2011.*

while handling sensitive personal data or information ("SPDI"). The IT Rules also strive to ensure that global data protection and privacy standards are met. However, the IT Rules have been criticised on grounds of ambiguity. The IT Rules define SPDI broadly to include various types of personal information. However, they are only applicable to body corporates or any person on behalf of body corporates. This excludes a significant portion of data collection and processing activities undertaken by individuals, partnerships, or entities other than body corporates. Further, while the IT Rules refer to service providers and other stakeholders, the obligations are only expressly imposed on body corporates. This fragmented approach dilutes the regulatory impact of the IT Rules. It allows a large portion of personal data processing activities to remain outside the purview of reasonable data security requirements mandated under the IT Rules. This substantively defeats the purpose of the IT Rules and reduces its effectiveness.

Another major criticism is that the IT Rules are not properly harmonised with other laws on data privacy in India, such as the various sectoral regulations on data privacy applicable to telcos, healthcare, etc. As an example, the IT Rules use a 'harm-based approach', regulating only sensitive personal data. On the contrary, unless exempted, regulations such as telecom industry privacy regulations automatically regulate all types of personal data. Such lack of harmonisation leads to overlaps, contradictions, and confusion regarding applicable standards. Data controllers and processors must adhere to varying standards under different rules for similar activity. This increases regulatory complexity and compliance costs. It also provides scope for arbitrage and forum shopping by data controllers seeking the most lenient regulations.[13]

Lastly, IT Rules doesn't provide for stringent penal consequences for violations. Rule 7 merely requires body corporates to 'define and periodically review' policies for breach notification and remedial action in the event of breach of privacy policies. It does not expressly impose any liability, damages, or penal consequences for non-compliance, breach or negligence by the body corporate itself. The only punitive provision is Section 43A of the IT Act, which provides for a maximum liability of Rs. five crores for negligent disclosure of personal information by a body corporate. This monetary cap of Rs. five crores is too lenient compared to the potential

[13] *Apar Gupta, Apar Gupta writes: Digital Data Protection Bill uses brevity and vagueness to empower government, undermine privacy* THE INDIAN EXPRESS *(Nov. 25 2022, 8:43 PM), https://indianexpress.com/article/opinion/columns/apar-gupta-writes-digital-data-protection-bill-brevity-vagueness-empower-government-undermine-privacy-827913/.*

scale of harm caused by data breaches, especially by large tech giants or social media companies processing data of millions of users. The effective deterrence is therefore absent. Recent occurrences, like as the Facebook-Cambridge Analytica scandal highlight the need for stronger penalties proportionate to the scale of entities and potential harm.[14]

2.2.2. Protecting Privacy: The Puttaswamy verdict

Judicial recognition of the fundamental right to privacy emerged from the Supreme Court's landmark Puttaswamy judgement in 2017, a watershed moment in Indian jurisprudence, emanated from the contentious backdrop of the Aadhar project and its implications on rights to life, liberty and freedom of expression.[15] It made an unequivocal declaration that the privacy right is a basic right under the Indian Constitution. This marked a shift from the earlier stance set by the M.P. Sharma and Kharak Singh ruling. In a collaborative effort, the court stressed that the privacy right is a necessary component of the right to life and personal liberty protected by article 21 of the Indian Constitution. The verdict went beyond the theoretical recognition of privacy as a basic right and delved into its nuanced applications. The state may impose reasonable restrictions on the right to privacy in its pursuit to achieve legitimate goals such as national security or public order. This constitutional underpinning established the expectation for robust data protection legislation that protects individuals' informational privacy.

2.2.3. Examination of the Personal Data Protection Bill, 2019

India's first standalone personal data protection bill was introduced in 2018, undergoing extensive debate and revision due to concerns over broad exemptions and inadequate safeguards.[16] An amended version, the PDP Bill, 2019, based on the Srikrishna Committee's recommendations, awaited Parliamentary approval amid further critiques of deficiencies compared to global standards. As legislative efforts continued, the government issued the joint parliamentary committee's report in December 2021, containing recommendations to address key gaps in the PDPB's rights protections.[17] Following that, on December 11th, 2019, the PDP Bill was presented in the Lok Sabha with the goal of setting up a statutory framework to govern the handling of personal data. The Bill attempts to find a balance individuals' privacy rights

---

[14] *Nicholas Confessore, Cambridge Analytica and Facebook: The Scandal So Far, ALJAZEERA (Mar. 28, 2018), https://www.aljazeera.com/news/2018/3/28/cambridge-analytica-and-facebook-the-scandal-so-far.*
[15] *Justice K.S. Puttaswamy, supra note 3.*
[16] *The Personal Data Protection Bill 2018.*
[17] *Joint committee on the Personal Data Protection Bill 2019, Report of the Joint Committee on the Personal Data Protection Bill 2019 (2021).*

and right to use data for innovation, by imposing obligations on entities processing personal data while exempting certain categories of processing from its purview. The Bill creates a three-tiered structure, imposing varying obligations upon data fiduciaries and processors depending on factors like: volume of data processed, risk of harm to the data principal, type of processing etc.[18] This calibrated approach helps balance innovation needs with data protection. For instance, "significant data fiduciaries" have added transparency and accountability norms.[19]

Though the bill has introduced certain pioneering concepts like significant data fiduciary, differentiated obligations, direct liability on data processors etc. which will enhance privacy safeguards, however, exemptions for government agencies from consent, transparency requirements[20], exclusion of non-personal data, automated decision making, absence of rights like right to be forgotten pose concerns.

2.2.4. Scrutinizing the Digital Personal Data Protection Bill, 2022

With the aim to regulate the processing of personal data of individuals in India and ensure their privacy and protection, the Digital Personal Data Protection Bill ("DPDP Bill"), 2022 contains a number of significant aspects.[21] The bill applies to all data fiduciaries and data processors, regardless of where they are incorporated or situated, as long as they process personal data in connection with any business conducted in India or profiling of individuals residing within Indian territory.[22] The definition of sensitive personal data is also expanded by the bill to include information about finances, transgender status, health, official identity, caste, religion, genetics, sex life, sexual orientation, biometrics, passwords, PINs, and other types of data that the government has designated as sensitive personal data. [23]

Even though the DPDP Bill, 2022 attempts to provide a legislative framework for the processing of personal data in India, the bill has received criticism on numerous fronts even

[18] *The Personal Data Protection Bill 2019, supra note 4, Chps III, IV, & VII.*
[19] *Id. § 26.*
[20] *Id. § 35, 12(a).*
[21] *The Digital Personal Data Protection Bill 2022, Preamble.*
[22] *Id. § 3.*
[23] *Id. § 3 (36)(A)-(M).*

before coming into effect.[24] Critics argue that the bill falls short on protecting privacy rights, obtaining meaningful consent, regulating children's data, ensuring accountability of companies, and having a wide enough scope.

A commonly cited limitation is the DPDP Bill restricting its scope to only personal data processed digitally or in digitized format.[25] This shrinks the landscape drastically as compared to laws like the GDPR. Excluding non-digital data would leave regulation ineffective for significant realms involving paper or physical records. There are also exclusions of personal data being processed by government entities that draw criticism. Such carve outs for entire sectors dilute the potency of the law and could enable abuse as per experts.[26] Even artistic and journalistic purposes have been exempted from consent requirements and transparency obligations.[27] While aiming to balance rights, critics argue the bill adopts too many blanket sectoral exceptions without sufficient safeguards.

III. THE NEWLY FASHIONED DATA PROTECTION LEGISLATION (DPDP ACT, 2023)

The Digital Personal Data Protection Act 2023 signifies a profound shift from India's historical reliance on industry self-regulation toward an enforcement-based regime anchored in individual rights. While the previous bills lack extra-territorial applicability, the DPDP Act, 2023 applies to Indian citizens and businesses that gather and use resident data. This also applies to any processing of digital personal data that occurs outside of India as part of any activity involving the delivery of products or services to Data Principals in India.[28] This legislation has taken significant steps in the localisation of data. While the 2019 bill prohibited certain data flows, the 2023 legislation only specifies that the government may restrict flows to specific nations through notification.[29] While not explicitly stated, the ability to restrict data

---

[24] *Anjali Bhardwaj, The problems with the Data Protection Bill, THE HINDU (Feb. 21, 2023, 12:15 AM), https://www.thehindu.com/opinion/op-ed/the-problems-with-the-data-protection-bill/article66531928.ece.*

[25] *The Digital Personal Data Protection Bill 2022, supra note 18, § 3(21).*

[26] *Anushka Jain, A public brief on the draft Digital Personal Data Protection Bill, 2022, INTERNET FREEDOM FOUNDATION (Feb. 16, 2023), https://internetfreedom.in/read-our-public-brief-on-the-draft-digital-personal-data-protection-bill-2022/.*

[27] *The Digital Personal Data Protection Bill 2022, supra note 21, § 17,18.*

[28] *The Digital Personal Data Protection Act 2023, supra note 5.*

[29] *Anirudh Burman, Understanding India's New Data Protection Law, CARNEGIE INDIA (Oct. 3, 2023), https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-*

transfers appears to provide the government with the authority it needs to pursue national security objectives. The bill further stipulates that this will not have an effect on steps taken by

sector-specific agencies that have or may have localisation obligations.[30] The Reserve Bank of India's localisation requirements, for example, will remain legally binding.

In contrast with preceding bills that exempted government agencies from certain provisions, the DPDP Act subjects both the private entities and the government to nearly identical data protection obligations. By holding the state to the same standards of transparency and accountability, the law signifies greater commitment to universal data privacy rights. Exceptions apply only where necessary for prompt action in the interests of sovereignty, security, friendly relations with foreign states, public order, and preventing incitement to commission of cognizable offences.[31] In enforcing accountability, the DPDP Act establishes a Data Protection Board of India ("DPBI") to ensure compliance, investigate violations and levy penalties. Whereas previous bills empowered multiple sectoral authorities,[32] the centralised DPBI is intended to enable more consistent, rigorous oversight. The revamped governance structure draws lessons from successful European regulators like Austria's Data Protection Authority.

The DPDP Act of 2023 establishes specific rights and duties for data principles. The rights include: right to access information regarding personal data, the right to correction and erasure

of personal data, the right to nomination, and grievance redressal.[33] The data principles' duties include: avoiding impersonating another person in certain circumstances, preventing the suppression of any material information, and not filing a fraudulent or frivolous grievance or

complaint, among other things.[34] Thus, by setting higher expectations of privacy protections, security safeguards, consent protocols, and transparency standards backed by stringent oversight and harsher penalties up to Rs 250 crores for non-compliance, the new law aims to effect a cultural change by placing user interests at the centre.

90624#:~:text=The%20law%20provides%20exemptions%20from,tribunals%2C%20or%20for%20the%20prevention%2C.

[30] *Id.*

[31] *The Digital Personal Data Protection Act 2023, supra note 5, Schedule II.*

[32] *The Personal Data Protection Bill 2019 (n 4) chp VII.*

[33] *The Digital Personal Data Protection Act 2023, supra note 5, § 11,12,13.*

[34] *Id. § 15.*

IV. INADEQUACIES IN THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Though the enactment of DPDP Act, 2023 has provided India the most awaited Data Protection legislation aimed at securing digital privacy, it has received numerous critiques on several aspects:

- Timeless data retention

While the DPDP Act requires reasonable purpose limitations and storage restrictions on collected data, it falls short of prescribing explicit time limits, unlike the GDPR which generally restricts storage to time durations necessary for specified purposes. Without precise retention cut-offs encoded in law, data mining, and unauthorised secondary usage may endure through exploits like broadly interpreted 'consent'.

- Transparency concerns

The act's transparency provisions have drawn criticism for excessive deference to commercial secrecy over public interest. While mandating algorithmic impact assessments and data audits, the law permits extensive redaction of these documents to protect intellectual property, hampering scrutiny of unfair, unethical or biased practices.[35] This negates the spirit of accountability.

- Exclusion of anonymized data

The act has excluded from its ambit anonymized data which appears to be a point of criticism of the recently revamped data protection legislation. It appears to be a point of concern as this data can be placed on top of personal data in order to draw inferences of the individuals.

- Ambiguous guidelines

The DPDP Act mandates the Data Fiduciaries to take reasonable security precautions in order to prevent breach of the Personal Data that it has in its possession.[36] However, the act fails to

[35] *Id. § 29(3), 37(5).*
[36] *Id. § 3 8(5).*

elaborate on as to what are these reasonable security measures leaving room for misinterpretation and misuse.

- Unregulated data usage

There are no restrictions on the utilisation or gathering of data under the data protection legislation. It allows data fiduciaries to collect data for any valid reason as long as it is lawful.[37]

- Harm Regulation

The act fails to mitigate harm pre-emptively and imposes no responsibility on the DPBI to inform citizens about their rights under data protection legislation.

- Unified data classification

The legislation includes no provision for classification of the personal data. All data is classified under one head i.e., digital personal data which refers to personal data in digital form.[38] It overlooks the fact that different types of data call for varying degrees of protection. As a result, sensitive and critical personal data are not adequately protected, necessitating stronger processing and retention guidelines.

- Exemptions granted to government entities

The DPDP legislation grants the government authority to process personal data of individuals without their consent on grounds of national security. This might result in superfluous retention of data leading to violation of privacy rights.[39]

- Concern on Board's independence

The central government is responsible for creation of mechanism for the selection and appointment of the data protection board's members. Additionally, the board members have a two-year term of office and are eligible for reappointment.[40] This raises concern over the board's independence from government's influence.

[37] *Id. § 2.*
[38] *The Digital Personal Data Protection Act 2023, supra note 5, § 2(n).*
[39] *Id. § 17.*
[40] *Id. § 20.*

- Lack of regulatory provision related to AI

The act lacks regulatory provision for regulation of data used and processed by Artificial Intelligence. This leads to unauthorised access of data potentially compromising the confidentiality and integrity of personal data.

- Voluntary undertaking

The act empowers the DPBI to accept voluntary undertaking from those who are not complying with the provisions of the act.[41] This constitutes a bar on the proceedings under the provisions of the act, providing wrongdoers with an opportunity to evade penalty.

- Improper handling of data

The DPDP Bill, 2022 held data fiduciaries accountable for wrongdoings committed by other data fiduciaries using shared data. This has been dropped in 2023 act, which resulted in inappropriate data management because it no longer requires data fiduciaries to secure the data principal's approval before sharing their data with another data fiduciary.

- Compensation oversight issue

The act states that all penalties collected from data fiduciaries goes to the consolidated fund of India. There is no provision to award compensation to aggrieved data principals.[42]

- No data portability right

The data portability right for data principals is not dealt with by the DPDP Act, 2023. By giving individuals an opportunity to choose from a variety of platforms, this right gave the data principals more power and promoted competition amongst data fiduciaries, which enhanced consumer welfare.[43] Although this right was mentioned in the 2019 PDP Bill, it is not present in the existing DPDP Act.

---

[41] *Id. § 32.*
[42] *Id. § 34.*
[43] *Trishee Goyal, How different is the new data protection bill, THE HINDU (Nov. 21, 2022, 10:57 PM), https://www.thehindu.com/sci-tech/technology/how-different-is-the-new-data-protection bill/article66166438.ece.*

Henceforth, it can be concluded that the recently enacted data protection legislation though marks a significant step in India's pursuit for a comprehensive and efficient data protection framework, a critical examination of the legislation indicates that it falls short on several fronts

and requires continued modification. Nevertheless, it remains a milestone first step, delivering enhanced accountability and remedies even if an incomplete realisation of data sovereignty.

V. POLICY RECOMMENDATIONS FOR STRENGTHENING DATA PROTECTION IN INDIA

In the wake of massive digital transformation across sectors, India needs an optimal approach to balance enabling data-driven innovation while still safeguarding citizen rights and preventing harms from unauthorized data collection or usage. Based on comprehensive analysis, the following recommendations could significantly enhance data protection in India:

- **Establishing an Independent Data Protection Authority:**

Though India has set up a data regulator i.e. Data Protection Board similar to authorities under the EU's GDPR or UK's Data Protection Act 2018,[44] there are concerns over the board's independence from government's influence. Such an authority being responsible to monitor and enforce compliance from public and private sector organizations collecting or processing personal data, investigate complaints, enable auditing mechanisms, recommending policy changes, its independence becomes a crucial factor to allow neutral oversight on issues like surveillance reform which it lacks currently. In order to ensure the freedom of the data protection board, the composition of the selection committee needs to be modified and made as diverse as was proposed in the 2018 draft of the bill, i.e. a judicial authority, an executive authority and external members.

- **Streamlining Consent Requirements:**

Current consent mechanisms for collecting personal data are fragmented or vague. A standardized and simplified framework for recording consent in line with global standards will enable users to fully understand data usage. Elements would include clear communication of

[44] *Graham Greenleaf, Global Tables of Data Privacy Laws and Bills, 8 SSRN 167, 168, (2023).*

purpose, storage periods, withdrawal procedures etc. Rules around child data consent also need strengthening. Making informed consent a primary ground for lawful processing while limiting dependence on vague grounds like is critical.[45] Extra protections are necessitated for processing sensitive data like financial information, religious beliefs, sexual orientation, medical records etc.

- **Limiting voluntary undertaking and providing compensation to the data principals**

There appears to be a need to limit the acceptance of voluntary undertakings from non-complaint entities by the Data Protection Board as it has become a mechanism to evade penalty. It needs to be made sure of that voluntary undertakings do not delay enforcement actions and a there is a requirement to establish clear criteria for evaluating the effectiveness of voluntary compliance measures. Furthermore, the DPDP Act, 2023 doesn't provide compensation to the data principals in case of breach. Allocation of a portion of the penalties collected form data fiduciaries towards compensation fund is required for the aggrieved data principals. It would lead to accountability and deterrence.

- **Facilitating Data Portability:**

Presently, citizens lack awareness or agency regarding data held by public agencies or companies about them. Procedural complexities also hinder portability rights. The DPDP Act, 2023 needs to introduce provisions for the right to data portability in order to empower data principles to transfer their personal data between different platforms and services, enhancing individual control over their data and promoting competition among data fiduciaries to improve consumer welfare. Competition and user control can dramatically rise once data portability between services becomes scalable like in the EU or Australia, without unreasonable denial grounds.

- **Instituting Safeguards for Government Surveillance & Use of Personal Data**

Controversies have erupted globally around how security agencies access citizen data from public or private sector databases lacking judicial or parliamentary oversight. Hence a robust assessment framework before authorizing security surveillance or government data access

[45] *Malcolm Dowden, Charmian Aw & Bindu Janardhanan, India Welcomes Landmark Data Protection law,* PRIVACY WORLD *(Jan. 29, 2024, 9:30 PM),* https://www.privacyworld.blog/2023/08/india-welcomes-landmark-data-protection-law/.

along defined grounds and quick redress for affected individuals will be pivotal. The DPDP Act 2023 needs to limit exemptions granted to government entities for processing personal data without consent on grounds of national security. It needs to implement strict oversight mechanisms and judicial review to prevent misuse and ensure compliance with privacy rights.

- **Incentivizing Privacy-Preserving Data Innovation**

As data-driven services evolve amidst growing digitization, concerns around intrusive data collection practices collecting excessive personal data also abound.[46] But privacy protection need not conflict with AI innovation for public good. Methodologies like federated learning, differential privacy, synthetic data etc. allow insights extraction without compromising sensitive raw data. Tax benefits, grants and related incentives can motivate startups and companies to integrate privacy enhancing techniques in product design. Voluntary adoption of global standards like ISO 27701 for sensitive data handling will signal positive industry orientation. Such approaches align well with the National Strategy for AI #AIforAll vision focused on responsible AI.[47]

With the national data protection policy taking shape, learning from global developments and India's unique socio-economic needs will inform balanced frameworks. User rights have to be the foremost benchmark though along with decentralized enforcement mechanisms. With apt policies, data-driven growth can positively transform lives across all sections while upholding informational privacy.

---

[46] *Amnesty International, Facebook and Google's pervasive surveillance poses an unprecedented danger to human rights, MEDIAWELL (Nov. 21, 2019), https://mediawell.ssrc.org/news-items/facebook-and-googles-pervasive-surveillance-poses-an-unprecedented-danger-to-human-rights-amnesty-international/.*

[47] *NITI Aayog, National Strategy for Artificial Intelligence #AIforAll (June 2018), https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf, (Last visited Feb. 2, 2024).*

VI. CONCLUSION

In its journey for a comprehensive data protection legislation, India has come a long way. From limited sectoral regulations under the colonial rule to the DPDP Act 2023, India has successfully achieved its much awaited and desired data protection legislation aligned with the global standards of individual rights and state duties. This watershed moment signals a cultural shift in India towards a privacy-centric governance. With the extra-territorial applicability, accountability, data localisation, rights and duties of data principles and data fiduciaries along with the gender diversity it brings, it truly serves as the guardian of the personal data of individuals.

While the DPDP Act 2023 signifies tremendous evolution from India's previous approach to data protection, the current legal regime continues to privilege commercial convenience over individual rights in key aspects. The act requires enactment of more precise, less discretionary standards and close loopholes permitting misuse under dubious pretexts like consent or commercial confidentiality in order to emerge as a truly empowering, rights-based framework.

However, its shortcomings should not discourage but encourage the policymakers to strive tirelessly for the continued development of the legislation, thereby making it efficient in resolving the developing concerns and leading to a robust data protection framework.