Impact Factor (SJIF): 6.092 E-ISSN: 2583-1615

International Journal of Research in Academic World

Received: 29/March/2024 **IJRAW:** 2024; 3(5):08-11 **Accepted:** 04/May/2024

Deciphering Right to Informational Privacy in India: A Comparative Analysis of DPDP Bill, 2022 and DPDP Act, 2023

[*1]Neha Agarwal

[*1]Research Scholar (UGC-SRF) and Teaching Assistant, Faculty of Law, Osmania University, Hyderabad, Telangana, India.

Abstract

The advent of digital age has prompted a need to shift focus beyond safeguarding the privacy of one's physical home. A new phenomenon of data-veillance has emerged due to widespread monitoring of people's actions using technology. The notion of informational privacy gained momentum in India with the recognition of right to privacy as a fundamental aspect of right to life under Article 21 by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India.* However, this judicial recognition was not accompanied by prescription of specific boundaries or mechanism for safeguarding data privacy. To overcome this challenge, this paper aims to identify safeguards to restrict arbitrary exercise of power by both state and private actors in the data-sphere. By undertaking a comparative analysis between Digital Data Protection Bill, 2022 (hereinafter referred as 'Bill') and Digital Data Protection Act, 2023 (hereinafter referred as 'Act'), this paper reviews whether a protracted period of consideration on the data protection law by the Parliament with relevant stakeholders has yielded into a robust law which not only safeguards personal data but also strikes a balance by addressing the necessity for lawful processes. To this end, the paper begins with an outline of key provisions of the Bill and Act and identifies trends of deviations between them. It proceeds with the evaluation of the Act on the anvil of the aforementioned four-fold proportionality test to demonstrate certain contentious aspects of the Act that may significantly diminish FRIP in India. The final segment proposes measures to overcome the legal conundrums surrounding the Act by employing 'Privacy by Design' framework within the law for it to withstand constitutional scrutiny.

Keywords: Informational privacy, privacy by design, accountability framework, data empowerment, proportionality test

1. Introduction

1.1. Evolution of a Fundamental Right to Informational Privacy (FRIP) in India

In a dynamic and swiftly changing digital environment, global headlines have frequently highlighted issues such as data protection and privacy concerns. The global phenomenon does not preclude India as its rapid transition to a digital economy is evident through a surge in internet connectivity wherein a staggering 300% increase is witnessed in last five years [1]. With the arrival of digital era, the emphasis on safeguarding privacy has necessitated a paradigm beyond protection from unreasonable search and seizure of one's home. This era is characterized by pervasive 'data-veillance' as individual's actions are systematically monitored using technology [2]. In this context, the concept of informational privacy has evolved from the assumption that all information pertaining to an individual inherently belongs to him and to be shared or kept private at his discretion. This right received impetus in India with the recognition of a fundamental right to privacy as inherent to right to life and that FRIP is encompassed within it by the Supreme Court in its breakthrough judgment in *Puttaswamy* [3].

The court recognized the three fundamental elements of informational privacy as 'secrecy', 'control' and 'anonymity' and held that such right is primarily concerned with safeguarding 'personal data' of a natural person. However, the court neither prescribed the specific boundaries of FRIP nor specific mechanism for safeguarding the right. This decision was followed by four iterations of proposed personal data protection Bills in the Parliament based on recommendations of Expert Committee headed by Justice B.N. Srikrishna and Joint Parliamentary Committee and after consultations with stakeholders. It culminated into the maiden Indian Act for data protection in 2023 after deliberations for over five years. Since the Act of 2023 is the second iteration of the Bill of 2022, the scope of the comparative analysis in this paper is restricted to these two versions.

1.2. Proportionality Test for Legitimacy of a Data Protection Law

Moreover, the court in *Puttaswamy* also recognized a 'four-fold proportionality test' to address the concerns regarding potential violation of right to privacy by the state as well non-state actors [4]. The test delineates the contours of a 'qualified right to privacy' by permitting state to impose reasonable restrictions on such right. The test mandates that:

i). The impugned action shall be authorized by a law;

ii). Such action has a legitimate aim in a democratic system;

***Corresponding Author:** Neha Agarwal

iii). Degree of interference through such action is proportionate to the necessity; and
iv). Procedural safeguards to prevent misuse.

The compliance of a prospective data protection law with the proportionality test not only infuses legitimacy to the law but also demonstrates its compliance with the principles of Rule of Law and Constitutionalism as state's discretion is restricted. On the other hand, a law which is non-compliant or violates any of the four-folds of the test shall invite constitutional scrutiny.

2. Proportionality Conundrum and Diminishing Data Privacy

2.1. Diminishing Ambit of Data Protection Law: The objective of both the Bill and Act is to regulate the handling of digital personal data in a way that respects the rights of individuals to safeguard their data while also acknowledging the necessity for processing for lawful purposes. However, the scope and application of the Bill and the Act varies. The scope of both extends to safeguarding only 'digital' personal data within Indian Territory when such data is collected in digital format or is subsequently digitized though initially collected in a non-digital format or when processing is outside Indian Territory but is linked to any activity involving offering of good or service to individuals within India. However, the Act excludes from its ambit the personal data which is voluntarily disclosed to the public [5] or extra-territorial data processing that involves profiling of individuals, which was under the purview of the Bill [6]. The Act fails to account for personal data which is automatically generated by third party especially through profiling from the publicly available data shared by individuals without the individual's assumed risk thereby diminishing the ambit of the Act especially in the face of mass profiling by social media platforms and technology companies.

2.2. Omissions in the Definition Clauses: While certain definition clauses are modified for an inclusive and effective enforcement of the Act such as inclusion of lawful guardian of a person with disability as Data Principal [7] and specific provisions under which Data Protection Officer, Data Protection Board (DPB) shall be established [8], certain key definitions that are essential for effective implementation of the data protection are omitted in the Act in comparison with the Bill such as 'harm' and 'public interest'. Further, both omits categorization of personal data into sensitive and non-sensitive.

The definition of 'harm' delineates a range of actions that are considered potentially risky to a data principal due to non-compliance of the law or data breach such as physical injury, alteration or identity theft, harassment or obstruction of legal or causing substantial loss [9]. In the absence of definition, the onus of proof on the data principal is onerous to prove harm against the data fiduciary. Further, the lack of definition of 'public interest' allows for usurpation and exercise of wide powers by the government for non-consensual data processing. This strikes at Rule of Law as it fails to fulfil the 'fair, just and reasonable' prong of the 'procedure established by law' under Article 21 as postulated by the Supreme Court in *Maneka Gandhi* [10]. Thus, it fails the first and third fold of the proportionality test as the Act allows state action in the absence of a law and fails to display that omission is proportionate to its actions under the Act.

2.3. Wide Exemptions and Discretionary Powers to the Government: The most contentious provision under the Act vis-à-vis the Bill is the considerable amount of discretionary authority to the government in the form of exempting certain entities and actions from the requirements of the law. It allows for exemption from obligations in specific circumstances when processing is for enforcing legal rights, under the orders of the court or tribunal, for prevention, prosecution or investigation of offences, necessary for a compromise involving amalgamation of companies, assessing financial data of an individual in default of payment, etc. [11]. Further, the law permits complete exemption from the ambit of law when processing is for safeguarding sovereignty and integrity of India, maintenance of public order and other restrictions under Article 19(2), research purposes and government notified data fiduciaries and startups [12]. Additionally, a significant discretionary power without clear guidelines allows government to declare that any provision of the Act will not apply to certain data fiduciaries within the five years of commencement of the Act [13].

2.4. Excessive Delegation and Broad Rule-Making Power: The Act vis-à-vis the Bill provides for excessive delegations of powers as it omits details of certain key provisions in the Act and instead empowers the government to prescribe these key provisions under the data protection rules. This provision goes against the established judicial principle of limited delegation. The delegated power encompasses how notices are issued to individuals, functioning of consent manager, procedure for reporting data breaches, obtaining parental consent for processing children's data, procedure for individuals to assert their rights and the appointment and operational procedure of Data Protection Board and Appellate Tribunal under the Act, to name a few [14]. With such wide rule-making powers to the central government, the regulatory intensity of the Act is considerably low vis-à-vis the Bill.

2.5. Displacement of Certain Rights of Data Principal: While both the Act and Bill recognizes the rights of data principal to access, correct and erase their personal data, the extent of the right has been restricted under the Act. The Act has restricted the extent of the right to access by specifying that data principals can access data only if they have consented to it beforehand. Moreover, the Act has eliminated the provision allowing the data principals to inquire about the stage of processing of their personal data. [15] They have failed to recognize two important participation rights such as data portability and right to be forgotten by displacing these rights from the earlier iterations of draft data protection Bills. Further, with respect to right to redressal of grievance, the timeframe of seven days provided in the Bill has been omitted and government is empowered to prescribe the time-frame under the Rules [16].

2.6. Lack of Independent Adjudicatory Mechanism: Concerns of Conflict of Interest: While the Bill is silent on the aspect of Appellate Tribunal under the adjudicatory mechanism, the Act designates Telecom Dispute Settlement Appellate Tribunal (TDSAT) under the TRAI Act [17] as the appellate tribunal to hear appeals

from the orders of adjudicatory officers under the Act [18]. TDSAT was set up to resolve disputes in the telecom sector and its competence to deal with violations under the data protection law is highly contentious. Further, TDSAT has been subjected to criticism for excessive governmental interference with its functioning since the enactment of the Tribunal Reforms Act, 2021 and the corresponding Tribunal Reform Rules, 2021. These reforms in tribunals have led to significant modifications wherein the government has broad discretion to prescribe the composition, appointment, removal, tenure and other related aspects of the chairperson and members through Rules.

Similar concerns of excessive governmental interference exist under the Act with respect to independence and autonomy of the Data Protection Board which acts as the primary adjudicatory body under the Act [19]. Additionally, the Act vis-à-vis the Bill eliminates the authority of the DPB to independently alter, suspend, revoke or annul its directions and makes it contingent upon referral by the central government [20]. Further, the Act eliminates the power of DPB to take action against data fiduciary for non-compliance. These aspects of an adjudicatory body which are touted as crucial to determine their independent functioning are left at the mercy of the government leading to conflict of interest as the government is also a data fiduciary under the Act [21].

3. Transition towards 'Privacy by Design' Framework

While some of the provisions of the Act are progressive and inclusive, it lacks procedural safeguards to comply with the proportionality test. To overcome this challenge, the paper proposes the following primary principles:

3.1. Accountability Paradigm: Shift in Onus of Proof and Strict Liability: To establish 'privacy by design' and address the aforementioned shortcomings in the Act, India's data protection law shall adopt an accountability paradigm wherein it obliges data fiduciaries to prove their organizational, technological and security capabilities towards safeguarding data privacy. To this end, the framework shall shift the onus of proof from the individual to data fiduciary to prove compliance with the law in case of a breach or non-compliance. This ensures that data privacy considerations are integrated in the Act by design from the beginning as it imposes accountability on all the data fiduciaries viz. state and private entities that are handling personal data. Further, under the proposed paradigm, in case of a breach leading to a potential 'harm to an individual', the tort principles of strict liability shall be imposed on the data fiduciary for their mishandling of personal data.

3.2. Amalgamation of Command and Control Model with Self-Regulation Model: The proposed paradigm shall imbibe the benefits of both command and control model under EU-GDPR as well as self-regulation model under certain US privacy laws wherein the former prescribes the principal legal framework which is multi-sector and technologically agnostic and the latter supplements it with a periodically updated model code of practices as recognized by the concerned industry standards. This leads to co-regulation and infuses adaptability in the law to stay abreast with emerging technologies and their potential intrusions to data privacy.

3.3. Legally Mandated Privacy Principles: A Guiding Force: As recommended by the Expert Committee headed by Justice A.P. Shah, the Act shall have legally mandated core principles in the form of national privacy principles to guide all the stakeholders of their rights and obligations under the Act especially in case of unforeseen circumstances or for navigating the grey areas of the law which is a real possibility in the technological arena. Such principles include collection limitation, purpose specification, storage restrictions, disclosure limitation, transparency and fairness in processing and data security along with clear and explicit notice and consent.

3.4. Recognition of Rights of Individuals for Meaningful Participation: For the Act to remain 'individual-centric', it shall adopt a rights-based approach that guarantees certain digital rights to all the individuals such that they can participate meaningfully in digital ecosystem. Such rights shall allow the individual to access the extent of personal data collected, correct such data in case of incongruences, erase their data subject to limitations, port their data from one fiduciary to another freely and right to address grievance along with the right to be forgotten. This shall concretize the contours of FRIP and allow individuals to exercise it in a way that not only assures privacy but also respect their autonomy and dignity.

3.5. Autonomous Adjudicatory Mechanism: The effective enforcement of any law is hinged upon the effectiveness of its adjudicatory mechanism which in turn depends on the ability of the body to remain autonomous. To comply with the fourth fold of the proportionality test, chairperson and members of both Data Protection Board as well as the Appellate Tribunal shall remain independent. The law shall prescribe the composition of the body and search-cum-selection committee for the appointment process, prescribe removal procedure, provide security of tenure, ensure salary and other allowances are fixed and not varied to the disadvantage of the members, place restrictions on post-retirement employment to ensure that both the bodies work without fear or favour and play a proactive role rather than being committed to the government. Further, the outer-limit on penalties in the Act may limit the power of the adjudicatory bodies and thus needs to be proportionate to the financial capacity of the organization, preferably, based on their annual turnover to create deterrence.

4. Conclusion

In India, there is a need for enhanced data protection and data empowerment wherein ordinary citizens including the marginalized groups are enabled to control their personal data to enhance their livelihoods. While the Act establishes a foundation, it alone is insufficient to ensure safeguard privacy in the absence of an accountability structure. To this end, the infusion of the 'privacy by design' framework within the law can ensure both protection and empowerment as it puts the onus on the data fiduciaries to prove their compliance and to respect the digital rights of individuals. The resultant framework shall rightfully acknowledge the right of informational privacy as an inherent fundamental right and also prescribe a mechanism to identify reasonable restrictions within the bounds of the constitution.

References

1. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1
2. NITI Aayog, *Data Empowerment and Protection Architecture* 24 (Aug. 2020), https://www.niti.gov.in/sites/default/files/2023-03/Data-Empowerment-and-Protection-Architecture-A-Secure-Consent-Based.pdf.
3. Y. McDermott, *Conceptualizing the Right to Data Protection in Era of Big Data*, Big Data and Society (2017).
4. Justice K.S. Puttaswamy, *supra* note 1.
5. *Id*. at pp. 71 (Justice D.Y. Chandrachud).
6. The Digital Personal Data Protection Act, 2023, § 3(c), No. 22, Acts of Parliament, 2023 (India).
7. The Digital Personal Data Protection Bill, 2022, § 4.
8. *Supra* note 6, at § 2(j).
9. *Id*. at § 2(l) and 2(c).
10. *Supra* note 7, § 2(10).
11. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
12. *Supra* note 6, at § 17(1).
13. *Id.* at § 17(2).
14. *Id.* at § 17(5).
15. *Id.* at § 5, 6(8), 8(6), 9, 11-14, 22-23 and 29(8).
16. *Id.* at § 11.
17. *Id.* at § 13.
18. The Telecom Regulatory Authority of India Act, 1997, §14, No. 24, Acts of Parliament, 1997 (India).
19. *Supra* note 6, at § 2(a).
20. *Id.* at § 18-20.
21. *Id.* at § 27.
22. Roger Mathews v. South Indian Bank Limited, (2020) 6 SCC 1.