Christ University Law Journal
2026, Vol. 15, No. 1, *99-126*
ISSN 2278-4322/https://doi.org/10.12728/culj.28.5

An Analysis of the Digital Personal Data Protection Act 2023

Sonia Nath* and Rumi Dhar†

Abstract

The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), is a significant step in India's efforts towards coherent and modern data protection. The Act is a statutory manifestation of the fundamental right to privacy affirmed in Justice *K.S. Puttaswamy v. Union of India*. The Act attempts to balance two competing necessities- the need to spur economic innovation and growth with the use of data, and the need to maintain the autonomy of persons in the digital or cyber sphere. The paper undertakes a critical study of the Act, considering key dimensions such as state accountability, independence of enforcement mechanisms, algorithmic transparency, and a regulatory role for emerging technologies such as AI, blockchain, and the Internet of Things. These dimensions are not only interrelated but also feed into one another, ranging from cross-border data transfers to surveillance exemptions and data fiduciary obligations. The paper puts the DPDP Act, 2023 in the context of broader privacy frameworks around the world and highlights that although the Act marks a normative development in data regulation, it also reveals enduring tensions in the pragmatics of regulatory governance. The paper concludes by proposing reforms, including the reintroduction of the Sensitive Personal Data, and ensuring robust regulatory protection for Artificial Intelligence and automated decision making, for effective implementation of the DPDP Act, 2023.

Keywords: Accountability, Algorithmic governance, Legal safeguards, Rights of individuals, Surveillance

1. Introduction

Data is one of the most important and valuable resources shaping governance, business and everyday social interaction in the contemporary digital age[1].

* Department of Legal Studies, Arunachal University of Studies, Namsai-792103, India; s.sonia.nath@gmail.com

† Department of Law, Nagaland University (a Central University), Lumami, Nagaland -798627, India; rumidhar@nagalanduniversity.ac.in

1 UNESCO, Data Governance in the Digital Age, https://www.unesco.org/en/data-governance-digital-age (last visited June 22, 2026).

In general terms, data are pieces of information used to represent facts, information, observations or records that can be collected, stored, processed, or sent using physical or electronic means[2]. It encompasses individual information such as biometric data, financial information, location data, communication data, online activity and more, as well as other data that is created digitally, in legal and technological terms[3]. Data is now hugely significant across the globe, especially in terms of its economic, social and strategic significance[4]. In the Indian context, the relevance of data has significantly risen with the growth of concepts and schemes like Digital India, Aadhaar, net banking, e-commerce and online Public service, which is characterised by the collection and processing of large volumes of sensitive data[5]. This increasing reliance on data-enriched technologies has also brought grave concerns about privacy, surveillance, cybersecurity, unauthorised disclosure, and misuse of personal information. In *Justice K.S. Puttaswamy v. Union of India*[6], the Supreme Court has reiterated the need for a comprehensive approach to provide a legal framework for personal data protection and accountability in the current digital environment in India[7].

Data in the digital era is a multi-faceted concept that can have technical, legal, commercial and cultural dimensions. At its most elementary level, data has been defined as a collection of facts, numbers, words, observations or other useful information,[8] while Merriam-Webster dictionary describes it as 'factual information, such as measurements or statistics, used as a basis for reasoning, discussion, or calculation, as well as information in digital form that can be transmitted or processed, and information output by a sensing device or organ that must be processed to be meaningful'[9]. In its simplest form, data is any information; it may take structured or unstructured form, and can be recorded, stored, processed and communicated. With the growing complexity of information systems, however, the legal and ethical question of who has, or has not, jurisdiction over data and its ownership has

---

2 Annie Badman and Matthew Kosinski, *What is Data*? IBM, https://www.ibm.com/think/topics/data (last visited June 22, 2026).

3 Council Regulation 2016/679, arts. 4(1), 4(13), 4(14), 9(1), 2016, O.J (L 119), 1 (EU), General Data Protection Regulation.

4 Yan Carrière-Swallow and Vikram Haksar, *The Economics and Implications of Data An Integrated Perspective*, IMF Departmental Paper No 19/16 (2019).

5 Lisa A. Hayes, Ctr. Democracy & Tech., *Digital India's Impact on Privacy: Aadhaar numbers, biometrics, and more,* (Jan. 20, 2015).

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

7 Justice K.S. Puttaswamy (Retd) v Union of India (2019) 1 SCC 1 (India).

8 Annie Badman and Matthew Kosinski, *supra* note 2.

9 *Data*, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/data (last visited June 25, 2026).

arisen[10]. Section 2(h) of the DPDP Act, 2023[11] defines data as a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means[12].

Personal Data refers to any data through which an individual is identifiable. Section 2(t) of the DPDP Act, 2023, 'personal data means any data about an individual who is identifiable by or in relation to such data'[13]. Sensitive Personal Data (SPD), although it is not explicitly distinguished in the DPDP Act, 2023, unlike the first draft bill of 2019, defines the term 'sensitive personal data as such personal data, which may reveal, be related to, or constitute- financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation'[14].

Non-Personal Data (NPD) refers to data that does not identify any individual and may consist of aggregated or statistical datasets. Although such data does not typically fall within the scope of privacy laws, its economic and strategic value has led to calls for a separate legal regime. The Committee of Experts on Non-Personal Data Governance, 2020 in India has just highlighted that it is necessary to monitor the NPD regulation for data sovereignty. The Committee of Experts defined Non-Personal Data as 'firstly, data that never relates to an identified or identifiable natural person, such as data on weather conditions, data from sensors installed on industrial machines, data from public infrastructures, and so on. Secondly, data that were initially personal data, but were later made anonymous. Data that are aggregated and to which certain data transformation techniques are applied, to the extent that individual specific events are no longer identifiable, can be qualified as anonymous data'[15].

Anonymised Data refers to personal data that has been processed in such a manner that individuals to whom it relates can no longer be identified, either directly or indirectly[16]. The process of anonymisation, therefore, serves as as critical mechanism for balancing the utility of data with the imperative of privacy protection.

---

10 Yan Carrière-Swallow and Vikram Haksar, *supra* note 4.

11 The Digital Personal Data Protection Act 2023, (No 22), Act of Parliament, 2023 (India).

12 The DPDP Act, 2023, *supra* note 10, § 2(h).

13 The DPDP Act, 2023, *supra* note 10, § 2(t).

14 The Personal Data Protection Bill 2019, No. 373, (2019), § 2(36), (India).

15 REPORT BY THE COMMITTEE OF EXPERTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK, MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOV'T OF INDIA, Dec. 16, 2020.

16 AEPD, 10 Misunderstanding Related to Anonymisations, (Aug. 08, 2025, 12 PM).

Digital data is information of any sort, be it written, visual, video or financial, that has been digitised. A key strength of digital data is that it can be reproduced, stored and reused so easily and is readily available for analysis. Economically, digital data is different when it becomes digital; it is 'non-rival', that is, many people can use the same data at the same time, meaning there is no depletion of the data resource, and 'non-excludable', that is, it is often difficult to prevent others from accessing or using the same data. The characteristics of digital data are[17]:

i. **Generative:** Data doesn't stop there; it's continuously generating new data. Whenever digital information is employed, it is able to produce digital information, knowledge, or patterns. It's a beginning that continually grows and changes with each use.
ii. **Replicable:** Digital data can be duplicated without error, and perpetually. Copies will generally be the same as the original, so it can be difficult to determine which came first.
iii. **Mixable:** Data is not confined to its original context. Data gathered for a specific purpose can serve a function beyond its original intentions.
iv. **Scalable:** Digital Data is very inexpensive to gather and store, and can be very large.
v. **Storable:** It is very easy to save all sorts of things rather than deciding what things to save.
vi. **Accessible:** It's something that everyone can use.
vii. **Persistent:** Digital information remains for an extended period of time (potentially indefinitely). Afterwards, it can't be completely erased.

Furthermore, digital data is often non-excludable, in the sense that it is inherently difficult to prevent third parties from accessing or using the same information. These characteristics, non-rivalry and non-excludability, bring digital data closer in nature to a public good, which has significant implications for how it is governed, shared and regulated.[18] Taken together, these properties set digital data apart from conventional economic resources and underscore the need for careful and considered frameworks governing its use.

This paper adopted both doctrinal and comparative research methodology. The doctrinal approach is used to analyse the provisions of the

---

[17] Digital Impact, *The Characteristics of digitized information require us to think carefully about how we use it as a resource*, https://digitalimpact.io/toolkit/digital-data/characteristics/ (last visited on 8th May 2025)

[18] Digital Impact, *The Characteristics of digitized information require us to think carefully about how we use it as a resource*, https://digitalimpact.io/toolkit/digital-data/characteristics/ (last visited on May 08, 2025)

DPDP Act, 2023, along with any judicial pronouncements and studies of the Constitution, laws and jurisprudence on privacy and data protection in India. The comparative approach is used to analyse international data protection frameworks and global privacy standards to broaden the evaluation of the strengths, weaknesses, and challenges involved in implementing the DPDP Act, 2023. The paper holds immense relevance in the present digital world, where the collection, processing and dissemination of personal data are directly related to governance and to business functions. The era of digitisation is fast-moving towards India, aiming to become a digital economy, and safeguarding personal data becomes all the more crucial. The extensive use of digital platforms and the high volume of data creation and transmission have inevitably led to a range of legal and ethical issues that deal with privacy and misuse of information.

The enactment of the DPDP Act, 2023[19] marks a watershed in the evolution of legal and constitutional recognition of data protection and digital rights in India. Emerging out of the historic Judgment of the Supreme Court in *Justice K.S. Puttaswamy v Union of India*[20] which recognised privacy as a fundamental right within Article 21 of the Constitution. The Court defined privacy as a compound right, involving bodily integrity, decision-making autonomy and information control. Importantly, it created the triple test of 'legality, necessity, and proportionality' of all infringement on this right and thus created a constitutional standard against which all data-related law must be judged.

Despite its progressive framing of data protection, the Act reveals a complex and contradictory regulatory framework that struggles to accommodate the imperatives of individual privacy and the requirements of a rapidly growing digital economy. The paper examines whether the provisions of the Act are consistent with constitutional principles of proportionality, transparency and state accountability and also considers the robustness of the institutional design, including the independence and efficacy of the Data Protection Board. The critical analysis places the Act in context as part of broader privacy regimes around the globe, particularly in the context of digital trade and the regulation of promising emerging technologies such as artificial intelligence, blockchain, and the Internet of Things.

1. Evolution of the Right to Data Protection in India

The journey of data protection in India highlights the slow move towards the acceptance of privacy and digital security as an integral part of the

[19] The Digital Personal Data Protection Act 2023, (No 22), Act of Parliament, 2023 (India).

[20] Justice K S Puttaswamy v Union of India (2017) 10 SCC 1, AIR 2017SC 4161.

constitutional framework in the country.[21] In the late nineties and early years of the new century, there was tremendous growth in technology and outsourcing business services, and there was a revelation of the importance of legal protection of personal and sensitive data[22]. Responding to this, the Government of India, in 1998, laid the foundation of the National Task Force on IT and Software Development to create strategies for the development of the country's information technology industry and the digital infrastructure[23]. Many of the suggestions from the Task Force influenced the Information Technology Act, 2000[24], such as the creation of cyber laws, cyber security and cyber governance through proper institutional mechanisms. The Act was, however, mainly about crimes of online transactions, and limited protection of personal privacy and rights to personal data. Act recognised crimes included hacking, breach of security, data theft, violation of privacy and the disclosure of information. Some rules were brought in, e.g. Section 43A[25] and Section 72[26], to provide limited protection for the security and privacy of data and impose responsibility for keeping data secure and a penalty for providing it without authorisation. The Act did not have a thorough mechanism for the collection, storage, and processing of personal data by public and private entities, which resulted in inadequate privacy safeguards. Other laws that helped data governance were the Credit Information Companies (Regulation) Act, 2005[27], which introduced regulatory provisions for the use of credit-related information. It highlighted responsible data collection, transparency, restriction of use, secure storage of financial information, and sanctions for infringing principles of privacy. India's formal acknowledgement of 'Sensitive Personal Data' was in the Information Technology Rules, 2011[28]. These rules brought consent-based data processing, privacy policies, reasonable security processes and grievance redressal mechanisms. While the Rules were limited in their scope, they had

---

21 Dr. Vikashdeep Singh Kohli and Kahondariya Jayeshbhai Talshibhai, *A Critical Review of the Right to Privacy in the Digital Age and Data Protection Laws in India*, 2 (1) Jagannath U. J Res. And Rev. 217 (2026).

22 Anirudh Burman, *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth*?, Carnegie India Working Paper (Mar. 2020).

23 The Information Technology Action Plan 1998, https://indiancabletv.net/itplan.htm#pre (Last visited Dec. 03, 2024).

24 The Information Technology Act 2000, (No 21), Act of Parliament, 2000 (India).

25 The Information Technology Act 2000, (No 21) § 43. Penalty and Compensation for damage to computer, computer systems, etc.

26 The Information Technology Act 2000, (No 21) § 72A- Punishment for disclosure of information in breach of lawful contract.

27 The Credit Information Companies (Regulation) Act 2005, (No 30), Act of Parliament, (India).

28 *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*, G.S.R. 313(E), Gazette of India, Apr. 11, 2011.

set in motion a few basic principles of transparency, accountability and data security, which paved the way for a modern approach to data protection in India and for future legislation such as the DPDP Act, 2023.

Apart from this, concerns were raised in the judgment of the *People's Union for Civil Liberties (PUCL) v. Union of India*[29] as the protection of personal information has grown increasingly important with the advent of the digital age, incidents of telephone tapping and telephone surveillance have increased. However, data protection in India experienced a turning point when, in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*[30] a nine-judge bench of the Supreme Court unanimously held that the right to privacy was a fundamental right and is deeply rooted in the right to life and personal liberty guaranteed under Article 21 of the Constitution of India. This decision not only treats privacy as a pure constitutional principle but laid down the ground rules for privacy protection in India, and that any violation of privacy by the state had to meet the triple test of legality, legitimate aim and proportionality[31].

The Supreme Court then gradually developed and clarified the meaning of privacy and digital rights in a series of landmark decisions. *Navtej Singh Johar v. Union of India*[32] was a case that not only decriminalised Section 377 of the Indian Penal Code, which criminalised consensual sexual relations between persons of the same sex, but also reinforced the principles of dignity, autonomy and identity as parts of the fundamental right to privacy, meaning that even the most intimate aspects of an individual's personal choice cannot be regulated by the state. Again, in *Joseph Shine v. Union of India*[33], the Supreme Court invalidated Section 497 of the Indian Penal Code, which criminalised adultery, as a direct violation of a woman's dignity and informational autonomy, concepts that form the basis of the privacy doctrine in *Puttaswamy*. Together, both these decisions illustrate the role of the right to privacy as a fence between the State and the individual, as well as between men and women.

In the recent case of *Anuradha Bhasin v. Union of India*[34], the Supreme Court had extensively deliberated on the constitutionality of internet surges in Jammu and Kashmir, thereby touching upon the digital aspect of the right to privacy. The Court ruled that freedom of speech and expression and freedom to engage in any trade, business and occupation through the

---

29 People's Union for Civil Liberties (PUCL) v. Union of India- AIR 1997 SC 568.

30 Justice K S Puttaswamy v Union of India (2017) 10 SCC 1, AIR 2017SC 4161.

31 *Id.* at 277.

32 Navtej Singh Johar & Ors. Vs. Union of India Thr. Secretary Ministry of Law and Justice- (2018) 7 SCR 379.

33 Joseph Shine v Union of India (2018) 11 SCR 765.

34 Anuradha Bhasin v Union of India & Ors (2020) 1 SCR 812.

internet are constitutionally protected rights and that any restriction on access to the internet must be both necessary and proportional and subject to judicial review. The judgment is especially relevant in the context of data protection because it recognised the internet as a fundamental tool in the enjoyment of digital rights, implicitly providing that any interference with the exercise of digital rights is an interference with privacy and informational autonomy. The Court also reiterated the protection of digital rights in *Dr. Sabu Mathew George v. Union of India*[35], where it gave guidelines for search engines to proactively block search results for pre-natal sex determination, which is closely linked with the new right to be forgotten and the principle of data minimisation.

The Supreme Court is now considering the balance between privacy and informational autonomy, and the Right to Information Act, 2005, (RTI) in the matter of *Venkatesh Nayak v. the Union of India*[36]. This case was filed in February 2026 as a public interest litigation (PIL) under Article 32 of the Constitution and raises a constitutional challenge against multiple provisions of the DPDP Act, 2023 and DPDP Rules, 2025. By noticing the matter, the Supreme Court has recognized that the petitioner has raised pertinent questions of law that require consideration, especially regarding the constitutional validity of the amendment to Section 8(1)(j) of the RTI Act by means of Section 44(3) of the DPDP Act which creates an unconstitutional restriction on the fundamental right to information guaranteed under Article 19(1)(a) and 21 of the Constitution[37]. The issue is on an expected hearing list for a tentative date of 07-08 August 2026[38]. The admission of this PIL itself matters a lot; it reflects constitutional recognition that data protection in India is not merely a legislative exercise but is founded in constitutional rights, and that the tension between a citizen's right to know and the State's expansion of the data protection regime requires careful constitutional analysis. This case will set a precedent for the delineation of transparency v privacy rights in India's constitutional framework. These decisions together formed the constitutional and jurisprudential basis for the creation of modern data protection legislation and gave impetus to the need for a broader data protection framework to govern personal data in a digital context.

3. Reports of the Experts Committee

The development of data privacy jurisprudence in India can be better understood by examining the recommendations of various expert committees

---

35 Dr. Sabu Mathew George v Union of India & Others – AIR 2018 SC 578.

36 Venkatesh Nayak v. the Union of India W.P.(C) No. 000177 / 2026.

37 Data Security Council of India, Case Brief: Venkata Nayak v Union of India- Re-examining Digital Personal Data Processing in India (2026).

38 Venkatesh Nayak v. the Union of India W.P.(C) No. 000177 / 2026, case status, Supreme Court of India case status portal, https://www.sci.gov.in/case-status-party-name/, (last visited June 26, 2026).

that have guided some of the significant legislative and policy moves in the field of data protection.

3.1. Justice A.P. Shah Committee Report, 2012

The Justice A.P. Shah Committee, established by the Planning Commission in 2012 to draft a model for privacy protection in India[39], was the first in a series of expert committee initiatives that paved the way for the developing data protection regime in India. Expert committees that made recommendations for comprehensive privacy laws in the digital age had a tremendous impact on the development of India's data protection framework. Justice A.P. Shah Committee Report in 2012[40] is one of the earliest and most important reports, which set the conceptual basis of Privacy/ Data Protection in India. The Committee addressed concerns with the increasing practice of and lack of accountability for the collection of personal information by both governments and private organisations, and noted that the current legal framework does not comprehensively protect this. It called for a more comprehensive privacy law to be passed, with several guiding principles, which included notice, consent, purpose limitations, accountability, and technological neutrality[41]. In addition, the report highlighted the multi-layered concept of privacy[42], the horizontal application of privacy duties to both government and non-government entities, and a co-regulatory approach to enforcement model, with Privacy Commissioners and Self-Regulatory Organisations[43]. It also put forward nine National Privacy Principles that would ensure that personal information is collected and handled with care, and would respect individual rights[44].

3.2. Justice B.N. Srikrishna Committee, 2018

One of the most significant developments in the history of data protection discussions in India was the report of the Justice B.N. Srikrishna Committee[45] prepared post the Supreme Court's landmark Judgement in *Justice K.S.*

---

39 Press Release, Press Information Bureau, Gov't of India, *Planning Commission, Group of Experts on Privacy Submit Report* (Oct. 18, 2012).

40 Planning Commission, Gov't of India, Report of the Experts on Privacy (Justice A.P Shah, Former Chief Justice, Delhi High Court, Chair, 2012.

41 Shah Committee Report, *Supra* note 69-76.

42 Shah Committee Report, *Supra* note 60-66.

43 Shah Committee Report, *Supra* note 56-59.

44 Shah Committee Report, *Supra* note 22- 27.

45 Committee of Experts on a Data Protection Framework for India, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, (Justice B.N. Srikrishna, July 2018), https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf (Last visited Dec. 23, 2024).

Puttaswamy vs Union of India[46]. The Committee aimed to develop a well-stabilised framework that would safeguard individual privacy while simultaneously fostering the digital economy in India. It brought to light new notions, such as 'data principals' and 'data fiduciaries', highlighting the principle of transparency, fairness, and accountability in how data is being utilised[47]. Furthermore, the report included essential rights like access, rectification, portability, and the right to be forgotten, and put forward obligations such as defining the purpose, minimisation, and notification of breaches[48]. It also called for an independent Data Protection Authority for proper enforcement and regulation[49].

4. Data Protection Bills

To understand the development of data privacy jurisprudence in India, it is important to review the different data protection Bills introduced over the years. The Bills are each a different phase in the process of evolving the legal framework, with different policy goals, constitutional values, stakeholder consultations and international best practices. These Bills provide a glimpse into the evolution of the legislation that led to the enactment of a comprehensive data protection regime in India.

4.1. Personal Data Protection Bill, 2019

The Personal Data Protection Bill, 2019,[50] was the first significant step taken in India to make a comprehensive legislation for the protection of personal data. Bill was a significant milestone in India's journey towards a comprehensive data protection regime. An analysis of this Bill will give us insights into the changing principles of data privacy jurisprudence in India, as it shows the response from the legislature to the constitutional developments, expert committee recommendations, and the need to regulate the processing of personal data in the digital age. The Bill came amidst the ongoing digitalisation process and stressed the importance of privacy as a right for all, highlighting the principles of transparency, accountability, and lawful processing of personal data[51]. It had suggested setting up a Data Protection Authority to oversee adherence to the regulations and standards[52]. The Bill put forward key tenets, which include consent, purpose limitation, data minimisation, storage limitations and rights to data access, data correction, data portability and the right to be forgotten[53].

---

46 Justice K. S. Puttaswamy v Union of India (2017) 10 SCC 1, AIR 2017SC 4161.

47 B.N Srikrishnan Report, Supra no 46, at 7 and 58.

48 B.N Srikrishnan Report, Supra no 46, at 51, 52, 54, 60, 62, 71, 75 and 81.

49 B.N Srikrishnan Report, Supra no 46, at 151.

50 The Personal Data Protection Bill 2019, Bill no 373 of 2019, (India).

51 PDPB 2019, *supra* note 47, §§ 4, 5, 10 and 23.

52 PDPB 2019, *supra* note 47, §§ 41, 42 and 49.

53 PDPB 2019, *supra* note 47, §§ 5, 6, 9, 11, 17, 18, 19 and 20.

4.2. Data Protection Bill, 2021

The recommendations of the Joint Parliamentary Committee[54], which studied the Data Protection Bill, 2019, resulted in the enactment of the Data Protection Bill, 2021[55]. It aimed to reinforce the framework of data governance in India, keeping in mind the concepts of privacy and national interest vis-à-vis digital innovation. The Bill called for a more comprehensive framework that would impact personal data as well as non-personal data, and stressed explicit consent, accountability, restrictions on surveillance and profiling, and data localisation[56]. It also clarified the obligations of data fiduciaries and processors, transfers of data across borders and how special categories of data, like children's data, would be protected[57]. As India started becoming more conscious about digital sovereignty and all-encompassing data regulation, the Bill took into consideration these aspects. The Bill represented India's increasing emphasis on digital sovereignty and comprehensive data governance[58].

4.3. Draft Digital Personal Data Protection Bill, 2022

The much-awaited Personal Data Protection Bill, 2019, was withdrawn from Parliament on 3rd August 2022 as the Joint Parliamentary Committee had proposed numerous amendments to the Bill, making a wholesale replacement of the Bill more pragmatic than a piecemeal revision of the existing Bill[59]. The Bill was also facing a lot of criticism due to its data localisation provisions, wide exemptions for government and its inadequate compliance with the evolving international standards of data protection[60]. In view of these limitations, the Ministry of Electronics and Information Technology published the Draft Digital Personal Data Protection Bill, 2022[61], for public consultation, which aims to build a comprehensive legislation to protect

---

54 The Report of the Joint Committee on the Personal Data Protection Bill, 2019, JCPDPB 2019, Seventh Lok Sabha, Lok Sabha Secretariat, Dec. 16, 2021, and laid in Rajya Sabha on Dec.16, 2021, https://prsindia.org/files/bills_acts/bills_parliament/2019/Joint_Committee_on_the_Personal_Data_Protection_Bill_2019.pdf (Last visited Dec. 23, 2024).

55 The Data Protection Bill 2021, (India).

56 DPB, *supra* note 52, §§ 2(A) (d), 11(3), 10, 3(23) ix-x and 33-34.

57 DPB, *supra* note 52, §§ 10, 16, 31 and 33-34.

58 DPB, *supra* note 52, § 49.

59 Anirudh Burman, *The Withdrawal of the Proposed Data Protection Law is a Pragmatic Move*, (Aug. 22, 2022).

60 Anirudh Burman, *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?*, Carnegie India Working Paper (Mar. 2020).

61 Draft Digital Personal Data Protection Bill 2022, Ministry: Electronics and Information Technology, PRS India, https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022 (last visited Dec. 25, 2024).

digital personal data in India. The Bill of 2022 aimed to rethink the legislative approach, with the introduction of the notion of 'deemed consent.[62] The Bill established the obligations of data fiduciaries and data processors in relation to the data principals, while also entrusting powers to data principals. It highlighted legal grounds for processing, data minimisation and limitation of data storage[63]. However, researchers have expressed concerns about the wide and vague exemption grounds in Clause 18(2)(a) of the Bill, which allows government agencies to be exempted from the provisions of the Bill without having to provide reasons, being open to misuse. Also, the state agencies' permanent exemption from the storage limitation requirements of Clause 18(4) was criticised as allowing for unchecked state surveillance and arbitrary infringement of citizens' fundamental right to privacy[64].

4.4. The Digital Personal Data Protection Bill, 2023

DPDP Bill 2023[65] introduced a comprehensive framework to help regulate personal digital data to ensure it is not only protected as private, but is also processed legitimately. The Bill outlined the rights and responsibilities of data principals and set forth various obligations for data fiduciaries to handle personal data responsibly[66]. The idea behind it was to increase accountability by imposing monetary fines for violations and promoting ease of doing business in the digital economy[67]. The foundational principles of the Bill are- Consent of the user, purpose limitation, minimisation of data, accuracy of data, storage limitation, security safeguards, and accountability[68], i.e., the principles understood and observed by governments around the world, which modernise India's existing data protection regime.

---

62 DPDPB, *supra* note 58, § 8.

63 DPDPB, *supra* note 58, §§ 10 and 11.

64 Hazaifa Shaikh & Dr. Radheshyam Prasad, Vacillating *Between No Law and Bad Law: An Analysis of the Digital Personal Data Protection Bill, 2022*, 12 NLIU L. Rev. 11 (2023), https://nliulawreview.nliu.ac.in/wp-content/uploads/2023/09/Vol-XII-Issue-II-11-29.pdf; PRS Legislative Research, Draft Digital Personal Data Protection Bill, 2022, https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022 (last visited Jan. 23, 2026).

65 The Digital Personal Data Protection Bill 2023, Bill no 113 of 2023, https://sansad.in/ls/legislation/bills (last visited Dec. 25, 2024).

66 DPDPB, *supra* note 62, §§ 4-10, and 11-15.

67 Ministry of Elecs. & IT, *Salient Feature of the Digital Personal Data Protection Bill, 2023*, Press Info. Bureau of India (Aug. 9, 2023), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1947264 (last visited Dec. 22, 2024).

68 PRS Legis. Research, The Digital Personal Data Protection Bill, 2023, PRS India, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited May 22, 2025).

Table 1: Key differences between various drafted Data Protection Bills[69]

The Draft Personal Data Protection Bill, 2018	The Personal Data Protection Bill, 2019	Recommendation of the Joint Parliamentary Committee	The Draft Digital Personal Data Protection Bill 2023
Scope and Applicability			
Processing of Personal Data. i) Within India ii) Outside India	Extends applicability to anonymised personal data	Processing of Personal and Non-Personal Data	Unlike the 2018 Bill, the new Bill removes references to business operating in India and no longer applies to offline personal data or non-automated data processing.
Reporting of Data Breaches			
The fiduciary's responsibility is to notify the Data Protection Authority of a data breach, and the Authority will review whether it is necessary to notify any data principal.	Same as the 2018 Bill	All breaches, regardless of potential harm, must be reported to the Authority within 72 hours	Every personal data breach must be reported to the Data Protection Board of India and each affected data principal.
Right to Data Portability and Right to be Forgotten			
Both rights were provided	Both rights were recognised	Both rights were recognised	Not included
Transfer of Personal Data outside India			
i) Every fiduciary must keep at least one copy of personal data stored in India.	i) A copy of sensitive personal data should remain in India.	Sensitive personal data will not be shared with foreign agencies without prior approval from the central government	i) No classification of sensitive and critical personal data.
ii) Personal data can be transferred outside India with consent, to approved countries, or under a contract authorised by the Authority	ii) About certain sensitive personal data, transfer is only allowed if it is made with specific consent.		ii) Personal data can be transferred if notified by the central government, subject to the prescribed terms and conditions.
iii) Certain critical data can be processed only in India.	iii) On critical personal data, as in the 2018 Bill.		

[69] PRS Legis. Research, Draft Digital Personal Data Protection Bill, 2023, PRS India, https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022, (last visited May 22, 2025).

5. Critical Appraisal of the Digital Personal Data Protection Act, 2023

The DPDP Act, 2023[70], represents a significant step towards India's endeavour to establish a comprehensive data protection regime seeking to balance individual data rights, the state's governance interests and the commercial and technological interests of the private sector. Yet, under its progressive movement, the Act has some conceptual, structural and procedural deficiencies. Through the multidimensional evaluation, the paper aims to see whether the DPDP Act, 2023, truly conceives of the constitutional promise of privacy or is primarily an act to fit in with the digital governance of India alongside economic compulsions. The key dimensions considered for critical appraisal of the Act are: (i) gaps in the provisions of the Act, (ii) gaps in the enforcement ecosystem under the Act, (iii) Cross-Border Data Transfer mechanisms, (iv) Algorithmic governance, (v) Data fiduciaries' duties and accountability, (vi) Rights of Data Principal, (vii) Regulation of Emerging Technologies, and (viii) Data localisation and breach notification.

5.1. Gaps in the substantive provisions of the Act

The DPDP Act, 2023[71], is the legislative action in the area of data governance in India. A close study reveals that there are some limitations to this Act. Firstly, it has conceptual vagueness where some key definitions are loosely defined. Secondly, it fails to adopt the tier of classification of data on the basis of risk-based protection, and thirdly, it grants blanket exemptions to the State.

5.1.1. Undefined core concepts

A legislation which covers fundamental rights must be clear and precise. This principle had been affirmed by the Supreme Court in *Shreya Singhal v Union of India*[72], wherein Section 66A of the IT Act was struck down on the grounds of vague terms in violation of Article 19(1) (a). The DPDP Act, 2023, much like the GDPR,[73] employs the term 'lawful purpose', without adequate definitional clarity[74], thereby conferring enforcement authorities and data fiduciaries excessive interpretative leeway. Without elaboration,

---

70 The Digital Personal Data Protection Act 2023, (No 22), Act of Parliament, 2023 (India).

71 *Id*.

72 Shreya Singhal v Union of India- AIR 2015 SC 1523.

73 Council Regulation 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directives 95/46/EC, 2016 O.J. (L 119)1.

74 Digital Personal Data Protection Act 2023, (No 22), Act of Parliament, 2023 (India) § 4 and see EU GDPR, *supra* note 69, art. 6(1) (providing a closed and exhaustive list of six lawful bases for processing, each precisely defined).

which can result in varying interpretations in each case, it will be difficult for individuals to be aware that their rights have been violated, as well as difficult for regulators to enforce compliance consistency. The General Data Protection Regulation of the EU contains ample technology-neutral definitions such as 'profiling', 'automated decision-making' or special categories of data. These had to ensure that the legal regime evolves with the changing digital risks. The Indian framework does not have this clarity, and therefore, a situation occurs where people are subjected to legal uncertainty, which is directly a violation of the requirement of clarity of law, which is part of the law concerning the fundamental rights.

5.1.2. Data Classification Tiers

One of the structural flaws of the DPDP Act, 2023, is that it refuses to categorise the personal data into risk-based categories such as 'personal', 'sensitive data' and 'non-personal data'[75]. Different kinds of data require different levels of protection depending on the risk that the data presents[76]. This not only differs from international best practices, but it also fails to consider what the judiciary is looking for when it comes to proportionality in the regulation of privacy[77]. The act treats all personal data identically, whether it is as innocuous as a person's name or as sensitive as their genetic information[78]. It makes the law weak to deal with domain-specific harm (e.g. in banking, health, fintech or AI-based profiling)[79]. This leaves a vacuum in terms of compliance and raises questions about whether harm mitigation is sufficiently addressed, particularly with the high-risk sectors. This one-size-fits-all model doesn't take into consideration the fact that some types of data breaches or misuse can be much more significant than others[80]. Without tiered

---

75 DPDP Act 2023, *supra* note 67, § 2(t) (defining personal data broadly as any data about an identifiable, without subcategories or risk-based tiers); see the Personal Data Protection Bill 2019, Bill no 373 of 2019 (India), § 15.

76 Committee of Experts on Data Protection, Ministry of Elecs. & IT, Gov't of India, A Free and Fair Digital Economy: Protecting Privacy, Empowering India (July 2018), (Srikrishna Committee Report recommended classification of personal data based on sensitivity and risk potential); also Council Regulation 2016/679, of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directives 95/46/EC, 2016 O.J. (L 119), recital 51, (recognised that certain categories of personal data are particularly sensitive and therefore deserve heightened protection).

77 EU GDPR, *supra* note 69, arts. 9 and 35.

78 DPDP Act 2023, *supra* note 67, § 2(t).

79 Daniel J. Solove, Data is What Data Does: regulating Use, Harm, and Risk Instead of Sensitive Data, 118 Nw. U.L Rev. 1081 (2024).

80 Samreen Ahmed and Mohammad Nasir, *Stakeholder Perceptions of India's Digital Personal Data Protection Act of 2023: An Empirical Study across Legal, Banking, and Corporate Sectors*, 11 Frontiers in Sociology: Sociology of Law (2026).

classification, the Act cannot implement proportionate safeguards, making it blind to the nuanced risk profiles of various sectors and technologies.

5.1.3. Unchecked State Power

The DPDP Act, 2023, has empowered the Central Government to exclude the State from the application of the Act, in whole or in part[81]. The Act provides two exceptions from the application of the Act. It exempts the processing of personal data, by any instrumentality of the State, for national security purposes, broadly interpreted as including the sovereignty and integrity of India, State security, foreign relations, public order or prevention of incitement to cognisable offences. Secondly, it applies the same exemption to the processing of any personal data by the Central Government from any instrumentality notified to it.[82]

These grounds are so broad and indeterminate (often couched in terms such as 'national interest' or 'sovereignty') that they give the executive broad powers of discretion that raise questions regarding the adequacy of safeguards against potential misuse and dilution of guarantees of data protection incorporated in the statute. Judicial decision in *Maneka Gandhi v Union of India*[83], where the Supreme Court held that 'procedure established by law' under Article 21 should be just, fair and reasonable. These safeguards do not find blanket exemptions from States under the DPDP Act, 2023. This creates an imbalance and allows the State to conduct surveillance outside the bounds of privacy law[84].

Section 17 of the DPDP Act, 2023 fails (i) as it confers unlimited power to the executive without putting in place any formal procedure[85], (ii) it is without necessity or proportionate assessments, and (iii) data subjects are left without any rights or redress against surveillance-driven violations[86].

5.2. Gaps in the enforcement ecosystem

A rights-based data protection regime is not possible without a strong, independent institutional framework. Laws alone do not ensure rights, but

---

81 DPDP Act 2023, *supra* note 67, § 17.

82 DPDP Act 2023, *supra* note 67, § 17 (2)(a).

83 Maneka Gandhi v Union of India- 1978 SCR 621, AIR 1978 SC 597.

84 Anirudh Burman, Understanding India's New Data Protection Law, Carnegie Endowment for Int'l Peace (Oct. 3, 2023).

85 Rudraksh Lakra, Medha Kolanu & Abhijit Shrivastava, Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023, 6 Global Priv. L. Rev., no 4, 2025.

86 Prof. (Dr) Vani Bhushan, Empowering Individuals: A Deep Dive into the Digital Personal Data Protection Act, 2023, 12 Int'l J. Advanced Rech. 891 (2024).

institutions do. The four interrelated institutional lacunae that cumulatively impact the enforceability of the Act are:

5.2.1. Institutional design of the Data Protection Board

One of the biggest loopholes in the DPDP Act, 2023 is in the form and functioning of the Data Protection Board of India[87]. The Central government is empowered to establish the Data Protection Board of India by notification in the Official Gazette[88]. The provision gives the Board the status of a body corporate, with perpetual succession and a common seal, and the legal capacity to acquire, hold, and dispose of movable and immovable property, and to contract and sue or be sued in its own name[89]. However, the Act grants the executive very broad powers to constitute the Board, such as control of what the Board is composed of and its functions, as well as how to appoint its members and what procedures to follow[90]. This concentration of control practically makes the Board an executive-dominated adjudicative authority, raising concerns about its institutional independence and its capacity to serve as an autonomous regulatory authority[91]. This gravely weakens the principles of independence, separation of powers and regulatory autonomy. The body does not possess many of the features that an independent data protection authority normally has[92]. In addition, the Board's role is somewhat limited to conducting the administrative inquiry, and it does not have some of the broader powers, such as making rules and providing policy advice, which are important for an effective and independent regulator[93].

5.2.3. Lack of Inter-Regulatory Coordination

Data protection in the 21st century is not a standalone regulatory function; it touches on areas such as fintech, health tech, telecom and AI governance. In India, these sectors are regulated by autonomous/semi-autonomous bodies such as the Reserve Bank of India (RBI), Telecom Regulatory Authority of India (TRAI) and National Health Authority (NHA). However, the DPDP Act, 2023 does not set up any formal mechanism for inter-regulatory decision-making and coordinated decision-making.

---

87 Abhishek Kumar, Prabhat Deep, Shivam Raghuvanshi and Vivek Kuma, *India's New Data Frontier: A Critical Legal Insight on the Personal Data Protection Act, 2023*, 44 Libr. Progress Int'l, no. 3, Jul.-Dec. 2024, at 11777.

88 DPDP Act 2023, *supra* note 67, § 18.

89 DPDP Act 2023, *supra* note 67, § 18(2).

90 DPDP Act 2023, *supra* note 67, § 18.

91 Software Freedom Law Ctr., India, Data Protection Board of India: A Watchdog Without Teeth, SFLC.in (Feb. 5, 2025).

92 Express Computer, Enforcement Gaps in India's DPDP Act and the Case for Decentralized Data Protection Boards, Express Computer (Jul. 4, 2025).

93 Anirudh Burman, Understanding India's New Data Protection Law, Car negie Endowment for Int'l Peace (Oct. 3, 2023).

The horizontal application of data protection law across sectors, including financial technology, health technology, telecommunications and artificial intelligence governance, has emerged as a challenge[94]. Each sector generates and processes personal data at an unprecedented scale and presents distinct legal, ethical, and regulatory risks. The data governance framework varies across sectors, with each having its own governing body: the Reserve Bank of India (RBI)[95] for financial services and fintech, the Telecom Regulatory Authority of India (TRAI) for telecommunications[96], and the National Health Authority (NHA) for digital health data under the Ayushman Bharat Digital Mission[97]. Despite this structural complexity, the DPDP Act, 2023, does not provide for any formal mechanism for inter-regulatory coordination or collaborative enforcement between the Data Protection Board and the sectoral regulators[98]. This regulatory vacuum can lead to overlapping compliance requirements and inconsistent enforcement.

5.2.4. Weak Grievance Redressal Framework

The DPDP Act, 2023 prescribes that complaints first should be submitted to data fiduciaries and thereafter, if not satisfied, then the same should be appealed to the Data Protection Board. In addition, the Act does not provide for a regional bench, ombudsman mechanism, legal aid provisions or digital grievance portals in regional languages, which makes the Act practically inaccessible for the rural and marginalised sections. Further, it lacks a clear appeal process to the judiciary regarding the decisions of the Data Protection Board of India.

---

94 Jidesh Kumar, *DPDP Act, 2023: Sector-Wise Impact on BFSI, Healthcare, E-Commerce, IT & Telecom in India*, Mondaq (Nov. 4, 2025), https://www.mondaq.com/india/data-protection/1700486/dpdp-act-2023-sector-wise-impact-on-bfsi-healthcare-e-commerce-it-telecom-in-india (last visited Feb. 26, 2023).

95 Reserve Bank of India, Reserve Bank of India (Digital Lending Directions, 2025, RBI/2025-26/36, DOR.STR.REC.19/21.07.001/2025-26 (May 8, 2025).

96 Telecom Commercial Communications Customer Reference (Second Amen dment) Regulations 2025, Telecom Regulations, 2025, No. 1 of 2025, Notification No. RG-25/(25)/2023-QoS (Telcom Regulatory Authority of India, Feb. 12, 2025).

97 National Health Authority, Draft Health Data Management Policy, Version 2.0 (Ayushman Bharat Digital Mission, Apr. 2022), https://abdm.gov.in/strapicms/uploads/Shefali_Malhotra_1eb4bacae4.pdf.

98 See Jidesh Kumar & Aurelia Menezes, *Cross-over with Sectoral Regulators under the DPDP Act, 2023: Harmonising RBI, SEBI, IRDAI, and TRAI Compliances*, King Stubb & Kasiva (Oct. 15, 2025), https://ksandk.com/data-protection-and-data-privacy/dpdp-sector-regulators-navigating-rbi-sebi-irdai-trai/, see also Interplay Between India's DPDP Act and Sectoral Regulators (RBI, IRDAI, SEBI, TRAI), DP India, https://www.dpo-india.com/Blogs/interplay-india%E2%80%99s-dpdp-act/, (Last visited June 29, 2026).

5.3. Cross-Border Data Transfer Mechanisms

The regulatory framework for how data is transferred across borders, as expressed through the DPDP Act, 2023, is a significant departure from previous calls for data localisation that were introduced in the 2018 draft Bill. Instead, the Act is very broad and vague, in which the Central Government will notify the list of countries or regions to which personal data can be freely transferred without outlining any specific standards of 'adequacy' or human rights protection. Most global data protection frameworks, such as the European Union's GDPR Article 45[99], allow the transfer of data across borders only when the recipient country provides an adequate level of data protection[100]. This mechanism provides legal certainty for businesses and ensures that citizens' rights are not diluted once their data leaves their borders[101]. The DPDP Act, 2023, however, does not have any such structured adequacy criteria[102]. There is also no reference to the need for reciprocal protections, judicial redress or independent mechanisms of oversight in the receiving country[103].

In the case of *Digital Rights Ireland Ltd v Minister for Communications*[104], the European Court of Justice struck down the Data Retention Directives, stating that mass data transfer without sufficient safeguards breached fundamental rights under the EU Charter. This establishes a precedent around the world that legality and adequacy are to drive cross-border transfer, an ethos that does not exist in the Indian construct. The absence of clear information-sharing parameters, transition timelines or adequate benchmarks brings with it legal and commercial risks.

5.4. Algorithmic governance

The DPDP Act, 2023, was anticipated to take care of the increasing role of automated systems in processing personal data.[105] However, the Act is silent on several important challenges of AI-driven decision-making[106]. It doesn't

---

99 Council Regulation 2016/679, art. 45, 2016 O.J. (L 119)1 (EU).

100 D.S Singh & Prerna, *Regulation of Cross-Border Data Flow and Its Privacy in the Digital Era,* 9 NUJS J. Regul. Stud. II (2024).

101 Smriti Parsheera, Data Protection and Cross-Border Data Flows in India, Brussels Privacy Hub Working Paper, Vol. 10, No. 5 (Mar. 2024).

102 Digital Personal Data Protection Act, 2023, § 16(1), No. 22, Acts of Parliament, 2023 (India).

103 *Supra* note 97.

104 *Digital Rights Ireland Ltd. v. Minister for Commc'ns, Marine & Nat. Res. & Others*, Joined Cases C-293/12 & C-594/12, ECLI:EU:C:2014:238 (Ct. Just. Apr. 8, 2014).

105 Rohit Jolly, Pranshu Singh & Aditi Kumar, *The Confluence of AI and Data Privacy: Aligning Data Privacy Regime in India for the Age of AI*, Bar & Bench (May 9, 2025).

106 Anurati Dasgupta & Ruchika Sharma, *Artificial Intelligence and Data Protection: Legal Challenges and the Need for a Robust Framework in India*, 13IJCRT (2025).

define or regulate profiling, fails to recognise any digital rights in the context of algorithmic harms, does not provide any protection from emotional and behavioural data exploitations and has no risk-based regulatory framework for automated systems[107].

5.4.1. Lack of Legal Safeguards for AI Profiling

Profiling means the use of personal data of an individual, including preferences, behavioural or mental health, reliability or economic status, through automated or semi-automated means. Despite the crucial role that profiling plays in automated governance, the DPDP Act, 2023 does not define, prohibit or regulate profiling. The European Union, GDPR, on the other hand, grants individuals the right not to be subjected to any decision that is being made solely based on automated processing[108]. The GDPR also requires transparency, impact assessments and justification mechanisms for such decisions[109]. In India, profiling has already developed in several domains. The NITI Aayog's National AI Strategy[110] advocates for AI in government, and public schemes such as Aadhaar-enabled Direct Benefit Transfer (DBT) and deployment of facial recognition technologies for automated surveillance and suspect identification[111]. However, this concern has not been converted into statutory protection. There is no mention of the right to explanation[112], the right to object[113], the right to meaningful human intervention[114], or the right to contest algorithmic decisions, which are increasingly recognised as important digital rights globally. In the global discourse on AI regulation, risk-tiered approaches are rapidly becoming the norm. The EU Artificial Intelligence Act 2024[115] categorises AI systems into 'unacceptable', 'high-risk' and 'limited risk' systems and prescribes a range of obligations to be placed on the latter. Such frameworks ensure that regulators prioritise resources and ensure a proportionality in enforcement. However, India's DPDP Act, 2023, does not mention the concept of algorithmic risk.

---

[107] Abhinav Singh & Dr Taru Mishra, Automated Profiling, Privacy Rights, and Gaps in India's DPDP Act 2023, 9 Iconic Rsch. & Eng'g J. 3521 (2026).

[108] Council Regulation 2016/679, art. 22, 2016 O.J. (L 119)1 (EU).

[109] Council Regulation 2016/679, art. 12, 13, 14, 22 and 35, 2016 O.J. (L 119)1 (EU).

[110] Nat'l Inst. for Transforming India (NITI Aayog), *National Strategy for Artificial Intelligence: #AIforAll* (2018).

[111] Mohita Yadav & Arti Sharma, *Facial Recognition Technology in India: Socio-Legal Debates on Privacy and Human Rights*, Int'l. J. Sci. Eng. & Tech. (2025).

[112] Council Regulation 2016/679, art. 13, 14 and 15, 2016 O.J. (L 119)1 (EU).

[113] Council Regulation 2016/679, art. 21, 2016 O.J. (L 119)1 (EU).

[114] Council Regulation 2016/679, art. 22, 2016 O.J. (L 119)1 (EU).

[115] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689) 1 (EU).

6. Data fiduciaries' duties and accountability

At the core of any credible regime for data protection is a well-defined set of duties for those entities that collect, process and monetise personal data-data fiduciaries[116]. These fiduciaries are both public and private, and are the primary custodians of the rights of data subjects. The DPDP Act, 2023, introduces the categories of 'data fiduciary' and 'significant data fiduciary'[117], which are conceptually inspired by the idea that persons handling personal data have a duty of care towards data principals. The obligations of 'data fiduciary' are imposed by virtue of Sections 7 and 8 of the DPDP Act 2023, which are procedural in form and are minimal in substance. Fiduciaries must get consent, have security safeguards and report breaches.

However, the DPDP Act 2023 does not require the fiduciaries to inform the individuals about how they will process their data, what algorithms are involved, and what will be, thus violating the audi alteram partem principle[118]. Data is not uniform in character; different types of data have different risks and sensitivity[119]. Similarly, various types of data impose different data handling practices with different concerns for law enforcement systems. However, the DPDP Act 2023 have a uniform set of fiduciary duties, without considering the risk diversity of different sectors[120]. Furthermore, the Act does not have inter-agency collaboration between the Data Protection Board and regulators such as RBI, SEBI, NHA or TRAI, leading to fragmented oversight[121]. The DPDP Act, 2023, fails to grasp this opportunity for harmonisation of regulatory gaps and lacks coordinated redressal mechanisms.

7. Rights of the Data Principals

The DPDP Act, 2023 presents a basic rights framework for data principals. The following are the lacunae in the empowerment framework under the Act:

---

116 Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. Davis L. Rev. 1183 (2016).

117 DPDP Act 2023, § 2(i) and (z), (No 22), Act of Parliament, 2023 (India).

118 Abhinav Singh & Dr Taru Mishra, Automated Profiling, Privacy Rights, and Gaps in India's DPDP Act 2023, 9 Iconic Rsch. & Eng'g J. 3521 (2026).

119 Daniel J. Solove, Data Is What Data Does: Regulating Vased on Harm and Risk Instead of Sensitive Data, 118 Nw. U.L. Rev. 1081 (2024).

120 DPDP Act 2023, §§ 7-10 (No 22), Act of Parliament, 2023 (India); Pushpit Singh & Silvia Tomy Simon, High Hope High Hurdles: Analysis of the DPDP Act and its Draft Rules (Part I), Int'l J. & Tech. Blog, NLS Forum (Jun. 8, 2025).

121 Jidesh Kumar & Aurelia Menezes, Cross-over with Sectoral Regulators under the DPDP Act, 2023: Harmonising RBI, SEBI, IRDAI, and TRAI Compliances, King Stubb & Kasiva (Oct. 15, 2025).

7.1. Incomplete recognition of individuals' rights

The DPDP Act, 2023 gives data principals a set of 5 core rights[122]- (i) the right to access personal data, (ii) the right to correct or erase inaccurate data, (iii) the right to nominate, (iv) the right to grievance redressal and (v) the right to withdraw consent. While these are necessary, they are insufficient in both scope and enforceability. In contrast, the EU GDPR ensures a much wider range of rights, such as the right to data portability[123], the right to object to processing, the right to restriction and rights against automated decision-making[124]. The most glaring omission in the DPDP Act, 2023 is the issue of data portability and the right to object to processing[125]. Data Portability gives people the power to move their personal data from one platform or service provider to another. The Right to object, on the other hand, allows users to challenge data processing that they believe is intrusive, unfair or excessive. These rights are necessary in the contexts of algorithmic profiling, targeted advertising and automated decision making.

8. Regulation of Emerging Technologies

The regulation of emerging technologies such as Artificial Intelligence (AI) and Blockchain technologies presents one of the pressing challenges for the contemporary legal framework[126]. These technologies are rapidly transforming the world and have the potential to significantly impact society, livelihoods, and economies. The future of the digital society is inextricably linked to such emerging technologies, from AI-driven decision-making systems to distributed ledger systems such as blockchain[127]. These technologies are not simply a tool that we use, but they redefine how data is generated, processed, circulated and acted upon. They also blur traditional legal distinctions between controller and processor, subject and object and even consent and interference[128]. A modern law on the protection of data must therefore be able to anticipate and adapt to changes in technology.

---

122 DPDP Act 2023, §§ 11-14, (No 22), Act of Parliament, 2023 (India).

123 Council Regulation 2016/679, art. 20, 2016 O.J. (L 119)1 (EU).

124 Council Regulation 2016/679, art. 21, 2016 O.J. (L 119)1 (EU).

125 Niharika Jaiswal & Dr Kavya Chandel, *Rights-First vs. Economy-First: A Compa rative Analysis of the GDPR and India's DPDP Act*, 6 Indian J. Legal Rev. 641 (2026).

126 Omena Akpobome, *The Impact of Emerging Technologies on Legal Frameworks: A Model for Adaptive Regulation*, 5 Int'l J. Resch. Pub. & Revs. 5046 (2024).

127 Yiwen Wang, *The Integration of Blockchain Technology and Artificial Intelligence: Innovation, Challenges, and Future Prospects*, 55 Applied & Computational Eng. (2024).

128 Hannah Ruschemeier, *Generative AI and Data Protection*, 1 Cambridge F. on A.I.: L. & Governance e6 (2025).

IoT systems generate data not through direct interaction with the user, via some kind of user input, but via sensors, wearable devices, home automation, vehicle telemetry and industrial monitoring (passive sensors)[129]. This data is often ambient, continuous and non-consensual in nature, and raises great concerns around opacity, control and intrusion of privacy[130]. However, the DPDP Act, 2023, does not cover device-generated data as a category on its own. It does not apply to the inferred and predictive data that IoT systems typically generate. Furthermore, blockchain systems are architecturally designed to ensure that once data is recorded on the chain, it becomes immutable and permanent, incapable of being altered, corrected, or deleted, a feature that functions as temper resistant decentralised ledger[131] The DPDP Act does not provide any information on how such rights may be exercised in a blockchain-based environment, which creates significant concerns for data subjects whose personal data may be recorded in the chain.

9. Data Localisation and Breach Notification

One of the most debatable aspects of previous drafts of India's data protection framework was the suggested data localisation mandates, requiring the storage of personal data in the territory of India. Justice B N Krishna Committee Report[132] had recommended a mandate for all personal data and strict localisation for critical personal data, emphasising data sovereignty, national security and law enforcement access. However, the DPDP Act, 2023 discarded the notion of a rigid localisation approach and instead adopted the model of transfer approval. There is no general obligation under the Act to keep or to process data within India exclusively[133]. Regarding data breach notification, a basic element of the contemporary data protection law is data breach notification, whereby breaches of data must be notified

---

129 Internet Society, IoT Privacy for Policymakers (2019).

130 Jens Kröger, *Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things*, in 548 IFIP Advances in Information and Communication Technology: Internet of Things, Information Processing in an Increasingly Connected World 102 (Leon Strous & Vinton G Cerf eds., Springer 2019).

131 Ammar Zafar, Reconciling Blockchain Technology and Data Protection Laws: Regulatory Challenges, Technical Solutions, and Practical Pathways, 11 J. Cybersecurity 1 (2025).

132 Committee of Experts on a Data Protection Framework for India, *A Free and Fair Digital Economy Protecting Privacy, Empowering Indians*, (Justice B.N. Srikrishna, July 2018), https://prsindia.org/files/bills_acts/bills_parliament/2019/Committee%20Report%20on%20Draft%20Personal%20Data%20Protection%20Bill,%202018_0.pdf (Last visited Dec. 23, 2024).

133 DPDP Act 2023, § 16, No 22 of 2023 (India); see Jidesh Kumar, *Cross-Border Data Transfer Under the DPDP Act and DPDP Rules, 2025: Navigating India's New "Navigating List" Regime*, (Apr.11, 2026).

in a timely and transparent manner so that people can take steps to protect themselves from harm[134]. The Act does not provide for a redress mechanism to appeal underreporting or delay. The breach notification mechanisms are not connected with the right to access, correction or erasure[135]. Thus, even in the event of a breach, data principals may not be provided with an adequate context from which they can assert or enforce their rights.

10. Limitations of the Digital Personal Data Protection Rules 2025

The Digital Personal Data Protection Rule 2025[136] was notified under the enabling provisions of Section 40 of the DPDP Act, 2023, and essentially provides the operational framework for India's data protection regime. These Rules possess an immense interpretative significance. They give shape to otherwise broad statutory provisions and form the backbone of compliance, enforcement and rights assertions under the Act. However, these rules also have some limitations, such as:

i. The wide scope of powers given to the Central Government, in particular under Rule 15[137] with reference to Section 16[138] on transfer of personal data outside India is a matter of concern as far as clarity and accountability are concerned. The rule does not explicitly define how such decisions are to be made or what safeguards are to be observed, particularly with regard to the transfer of personal data to any foreign[139].

ii. Rule 7[140], which deals with the intimation of personal data breaches, is a reasonably structured concept where Data Fiduciaries shall be required to send intimation to the Data Protection Board and concerned Data Principals without undue delay and in any case within seventy two hours of coming to notice of the breach. The rule also explains the type of information that needs to be disclosed, such as the circumstances of the breach, what mitigation steps have been taken, and what steps to

---

134 Anirudh Burman, Understanding India's New Data Protection Law, Carnegie Endowment for Int'l Peace (Oct. 3, 2023).

135 Digital Personal Data Protection Rules, 2025, r 7, G.S.R. 869 (E), Gazette of India, Extraordinary, Part. II, Section 3(i) (Nov. 13, 2025) (India).

136 Digital Personal Data Protection Rules, 2025, Gazette of India, pt. II sec. 3(i) (Nov. 13, 2025) (India).

137 Digital Personal Data Protection Rules, 2025, r 7, G.S.R. 869 (E), Gazette of India, Extraordinary, Part. II, Section 3(i) (Nov. 13, 2025) (India).

138 DPDP Act 2023, § 16, No 22 of 2023 (India).

139 Can You Transfer Data Outside India*? DPDP Rule 15 Explained*, Privacy Global (2026).

140 *Supra* note 132.

take to prevent it from happening again. Penalties for failure to notify are provided for under the Schedule to the Act, but Rule 7 does not provide for any minimum penalties for delayed notification and does not make any clear attempt to link breach notification with access to remedies for affected persons[141].

iii. Rule 14 provides for modalities on how data principals can exercise their rights (including access and correction). However, the right to data portability, automated decision and collective redress is missing, and there is no timeline for fiduciary compliance with user requests.

iv. Rule 15[142] allows data transfer outside India unless the Central Government prohibits such data transfers by order. However, there is no proper evaluation process of adequacy, no reciprocity clauses, and no multilateral guarantees of compatibility.

v. Rules 17-21[143] determine the composition, functioning and digital interface of the Data Protection Board. While the emphasis on online proceedings is forward-looking, the institutional design has the following shortcomings: (i) no tenure protection for Board members, (ii) Selection Committee dominated by Executive Secretaries, and (iii) lack of judicial oversight in the appointment or removal.

11. Conclusion

The DPDP Act, 2023 is an important step in the right direction as far as India's effort to regulate a rapidly changing landscape of digital life is concerned. It introduces a long-awaited legal framework for personal data, consent mechanism, notice and fiduciary responsibility and procedural safeguards. Yet, as this paper critically reveals, the DPDP Act, 2023, lacks in some respects. The analysis has identified multiple structural limitations, from vague definitional frameworks, exemptions controlled by executives, minimal procedural safeguards, and the absence of algorithmic rights, institutional independence and sectoral regulations. After the comparison of the DPDP Act, 2023, with other data protection laws across the world, it makes one understand how other jurisdictions have better embedded data dignity and algorithmic transparency. As emerging technologies such as AI, IoT and blockchain change the landscape of data flows and control, the

[141] Sumit Kumar, India's DPDP Enforcement Framework: The Remedy Gap, Mediation Route and Independence of the Data Protection Board, TLC Tax Law (June 2026).

[142] Digital Personal Data Protection Rules, 2025, r 15, G.S.R. 869 (E), Gazette of India, Extraordinary, Part. II, Section 3(i) (Nov. 13, 2025) (India).

[143] Digital Personal Data Protection Rules, 2025, r 17-21, G.S.R. 869 (E), Gazette of India, Extraordinary, Part. II, Section 3(i) (Nov. 13, 2025) (India).

need for a second-generation data protection framework becomes apparent. In sum, the DPDP Act, 2023, is a beginning and not an end yet. The analysis throws up the promise and dangers of India's digital data governance framework.

The passage of the DPDP Act, 2023 and the Rules 2025 mark India's formal embrace of the era of data governance. However, the paper has shown that the existing regime is marked by limited articulation of rights, executive-dominated institutions and a compliance-oriented philosophy with a form-oriented, rather than substance-oriented approach to the law. The recommendations are proposed in this connection:

11.1. Institutional Innovation and Structural Reforms:

The effectiveness of any data protection regime rests not just in rights or rules, but in the institutions that interpret and embody those rights and rules. The existing Data Protection Board does not have the independence, transparency, and diversity to serve as a counterbalance to state and corporate power. There is a need to develop a multi-tiered grievance redressal structure that includes:

i. Regional breach reporting and digital accessibility
ii. The ombudsman model that is empowered to make binding orders
iii. Mandated coordination with the sectoral regulators (RBI, TRAI, NHA, etc.) through Joint Regulatory Committees

11.2. Risk-Based and Rights-Based Processing System:

Processing of data cannot be controlled following static or uniform rules. Instead, it requires a risk and context-sensitive system, which matches compliance obligations with the sensitivity of the data and the scale of impact and vulnerability of the data subjects:

i. Classification of data according to Risk

   Tier I: Basic identifies (i.e. name, contact)

   Tier II: Sensitive Personal Data (e.g., health, financial, religion, etc.)

   Tier III: High-risk information (e.g. biometric, emotional, behavioural

ii. **Risk** assessments that include the use of algorithms should include mandatory AI impact assessments to carry out a systematic assessment of the potential harm, bias and risks to the rights of individuals. In addition, people should be given an explicit right to opt-out of algorithmic profiling, thus giving them greater control over the way automated systems handle personal data and make decisions that may have a significant impact on them.

11.3. Enforcement Ecosystems:

The Data Protection Board of India is a quasi-independent authority that adjudicates upon data breaches and imposes penalties. This model destroys institutional autonomy. Comparative models such as the EU Data Protection Board and the UK Information Commissioner's Office operate with more independence. Further, this can be improved by Statutory Independence of the DPBI and empowering the Board to make binding codes of practice and frameworks for emerging technologies.

The Data Protection Board of India is a quasi-independent authority that adjudicates upon data breaches and imposes penalties. This model destroys institutional autonomy. Comparative models such as the EU Data Protection Board and the UK Information Commissioner's Office operate with more independence. Further, this can be improved by Statutory Independence of the DPBI and empowering the Board to make binding codes of practice and frameworks for emerging technologies.

11.4. Cross-Border data transfer:

The Act follows a government-notified whitelist approach, which means that personal data transfer is permitted only to countries approved by the Central Government. Existing cross-border frameworks for data transfer are needed:

i. Building a risk-based adequacy model to replace the whitelist model
ii. Introducing Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs) for ensuring interoperability with the global data ecosystem
iii. Digital Trade Facilitation Agreements to avoid barriers to data localisation and guarantee privacy protection

11.5. Algorithmic Transparency and Automated Decision-Making (ADM):

ADM profiling and algorithmic bias are currently silent in the DPDP Act, 2023. Without algorithmic transparency policies in place, people do not have a right to explanation or object to AI-driven profiling. So, there is an urgent need to

i. Introduce a 'right to explanation' for decisions made through automated processing. The right entitles an individual to receive a clear explanation whenever a consequential decision is made about them using automated processing.
ii. Mandate Algorithmic Impact Assessments (AIA) and human oversight to identify the risk of bias, discrimination and harm before the system

is operationalised. All high-risk automated systems must undergo AIAs carried out by independent auditors. There should also be meaningful human oversight, and no automated system should make final decisions regarding individual rights without human oversight.

iii. Organisations are required to disclose the source and categories of data used to train AI models, as well as actions taken to identify and mitigate bias.

While the DPDP Act, 2023, marks a pivotal milestone in India's data protection landscape, it fails to address automated decision-making and algorithmic accountability, creating an ever-expanding disparity between the law and the technology that people face in their everyday lives. These challenges need to be tackled proactively by adopting international best practices and tailoring them to the Indian context, to ensure that the vision of a rights-centred digital ecosystem is brought meaningfully to the era of artificial intelligence.