Delhi Metropolitan Education
Affiliated to GGSIP University, New Delhi & Approved by Bar Council of India

RESEARCH ARTICLE
doi: 10.53361/dmejl.v6i02.02

The Digital Personal Data Protection Act, 2023: Key Provisions, Issues, and Future Directions

Manindra Singh Hanspal*

Assistant Professor, Presidency University, Bengaluru, Karnataka, India

Abstract

The Digital Personal Data Protection Act, 2023 is a necessary step towards safeguarding the data privacy in India where quick digitalization is in progress. With the growing prevalence of personal data breaches and cyber threats, the Act's role in resolving these issues is primary. This study is a critical review of the DPDP Act, its main provisions, the challenges encountered in its implementation, and potential future developments to enhance the Act. The paper employs a comparative legal methodology, focusing on the Act's provisions, enforcement mechanisms, and weaknesses. It relies on research into the doctrines and a critical analysis of applicable case law to assess the Act's success in ensuring data privacy and the practical difficulties it faces. The results reveal several acute problems, including gaps in enforcement, government exemptions that narrow the statute's scope, and concerns about data localization requirements. Nonetheless, the Act's benefits for data subjects are evident in its provisions, including those on informed consent and data access. Although the DPDP Act provides an adequate legal framework for data protection, it still needs to be refined to align with emerging technologies, including AI and blockchain. The further revisions must address enforcement challenges and make the Act more global and effective in the context of rapidly changing digital environments. This paper highlights the need to continually revise it to protect individuals' privacy and build confidence in the Indian digital landscape.

ARTICLE INFO

***Correspondence:**
mhanspal21@gmail.com
Assistant Professor, Presidency University, Bengaluru, Karnataka, India

Dates:
Received: 18-07-2025
Accepted: 20-10-2025
Published: 31-12-2025

Keywords:
Data Privacy, Legal Framework, Personal Data Protection, Privacy Law Enforcement, Digital Transformation

How to Cite:
Hanspal MS. (2025) The Digital Personal Data Protection Act, 2023: Key Provisions, Issues, and Future Directions. DME Journal of Law, 6(2), 12-23.
doi: 10.53361/dmejl.v6i02.02

Introduction

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a landmark in the history of the Indian legal system to deal with the rising issues of data privacy and cybersecurity in an ever-digitized world. As India is rapidly becoming digital with more than 86 percent of all households currently linked to the internet, cyberattacks, data breaches, and misuse of personal information are on the increase. The number of cybersecurity events in India had soared to 22.68 lakh in 2024 as compared to 10.29 lakh in 2022, which highlights the dire need to have tough data protection laws and their effective enforcement.[1] The DPDP Act such as the law focused on supporting the privacy of the data of the citizens will be central to developing the proper legal framework of the collection, processing and storage of personal data in keeping with other standards in the field, including the GDPR (the General Data Protection Regulation) but applied

DME
Journal of Law

to the Indian context. The last ten years have seen the swift development of digital transformation in India, which has increased data-gathering, storage, and transfer speeds many times across different platforms, posing serious privacy, misuse, and unauthorized access issues. These issues have been brought to public attention, and nowadays people have made data privacy a central point in legal, social, and political debates. The purpose of adopting the DPDP Act is to address these issues by granting individuals additional rights over their personal data and making data processors responsible for breaches of these rights.

It is a global trend that data protection laws continue to gain importance. Since nations like the European Union are first to implement the General Data Protection Regulation (GDPR), other nations have attempted to establish similar sources of law to safeguard the information of people in the era of digital technologies. The DPDP Act formerly the Data Protection Bill was created in India and formulated based on the global trends as well as the mounting pressure exerted by national digital protection challenges. The Indian government initially structured data protection on a piecemeal basis.[2] However, the framework has now been replaced by the DPDP Act, which offers an extensive legislative framework to address the same. The multiple aspects of data protection in India have already been discussed, particularly the role of the Puttaswamy case (2017), which established privacy as a constitutional right.[3] The latest discussions of the DPDP Act have raised concerns about exemptions for government entities and the data localization provision, both of which may undermine the Act's efficiency.[4] In addition, international comparisons, particularly the GDPR, indicate that, although the DPDP Act has some features similar to international standards, it lacks certain features associated with the right to be forgotten and the data portability.[5]

Knowledge Gap

Even though the literature on the data protection framework in India is on the rise, the literature has not undertaken a critical review or overall examination of the difficulties in its operations and the practical implications of the DPDP Act. A significant part of the literature concerns theoretical considerations of the law or its comparison with international law. However, fewer studies address the Act's effectiveness in practice and the possibility of modifying it to accommodate future technological changes.

Rationale & Novelty

The research is necessary since it gives a detailed overview of the provisions of the DPDP Act and examines how the Act applies to digital transformation in India. Although other research has assessed various elements of the law, few have provided an extensive critique that covers both the law and its challenges. The paper integrates doctrinal and comparative research findings to provide a comprehensive assessment of the DPDP Act's strengths, weaknesses, and potential areas for improvement. It also highlights the lack of full consideration of emerging technologies (AI and blockchain) in existing provisions, underscoring the need for future legislative changes.

Legislation History and Background

Background of the DPDP Act

The Digital Personal Data Protection Act, 2023 (DPDP Act) has been a landmark in the Indian quest to have sound legislation on data privacy. Both the local law trends and the global data protection regulations have had a significant impact on the journey. The Puttaswamy case (2017)[6] in India further increased the rate of data privacy, since the Supreme Court of India had identified the right to privacy as a right of fundamental importance under Article 21 of the Constitution.[7] The case was a landmark and formed the basis of the legislative process that culminated into the enactment of the DPDP Act. The case brought out the constitutional need to safeguard the personal information of individuals in the wake of fast digital transformation. The second step that was significant was the case of Shreya Singhal (2015)[8] which concerned the freedom of speech and internet. The case, even though not directly concerning data protection, has brought a vital concern regarding the concept of regulation versus personal freedom in the internet space.[9]

This case decision was a pointer to the necessity of rigorous and explicit legislative frameworks concerning the problems of digital rights and freedoms including data privacy. These pioneer cases led to the intensification of the discussion surrounding the need to have data protection laws and the Personal Data Protection Bill, 2019, was written.

Impact of International Norms

The international data protection rules had a significant impact on India as the country formulated the DPDP Act, particularly the European Union data protection regulations otherwise known as GDPR and the California Consumer Privacy Act (CCPA).[10] Both standards, the GDPR and CCPA, establish very high requirements in the processing of data and consumer rights, providing severe conditions of informed consent, the movement of all data in its entirety, and the constant information of consumers about data breaches.[11] A great number of these principles may be incorporated into the DPDP Act, including express consent to the collection and treatment of data, the right to access and delete personal data. As to GDPR, the DPDP Act is concerned with data minimization, i.e. collecting and retaining only the necessary data.[12] Nevertheless, whereas the GDPR is reported to be comprehensive in its application to personal data across various domains, the Act in India has been modified to address the particular issues of the Indian digital environment, including state exemptions and the perceived issue of data localization. In contrast to the CCPA, which prioritizes consumer rights within the Californian economy, the DPDP Act focuses on protecting personal data in a developing economy with its own peculiarities, such as a lack of digital literacy and infrastructure.[13]

Previous Drafts and Bills

The Personal Data Protection Bill, 2019 has proven to be the most significant challenge faced by the history of the DPDP Act, in its multiple drafts. The Bill was initially proposed by the government in order to provide a broad data protection legislation in the digital age. The Bill of 2019 included the clauses that were in line with the GDPR, such as the right to be forgotten and notification of data breaches.[14] Critics, however, claimed that the law had far-reaching exemptions for government agencies that could compromise its effectiveness. One of the significant areas of debate in the Bill was the question of domesticating data. The opponents stated that the Bill's clause requiring companies to store information in India may negatively impact foreign businesses and global information flows. These issues led to the addition of provisions in the DPDP Act to balance national security requirements with the interests of the digital economy.[15]

There have been many revisions to the 2019 Bill, informed by the recommendations of multiple committees, including the Srikrishna Committee and the Parliamentary Standing Committee on Information Technology. The result of these revisions was the DPDP Act, which exhibited a more developed view of data protection, with stricter enforcement mechanisms, better-defined individual rights, and a more focused structure of data fiduciaries. The historical chronicle of DPDP Act- starting with the Puttaswamy and Shreya Singhal cases up to the enactment of the Act, elucidates why it is necessary to create a law on data protection that does not merely safeguard citizen privacy, but also regarding the socio-economic background that India is running in.[16]

Structure and Major Provisions of The DPDP Act

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a useful act that is designed to protect the personal information of people in India. The government signed the Act on August 11, 2023 and is looking forward to its final implementation in phases with the enforcement coming soon.[17] The DPDP Act answers the main questions concerning the privacy, security, and accountability of data and can be compared with the international standards like the GDPR.

Outline of the Organizational Structure of the Act

The DPDP Act consists of six key chapters having particular coverage of the law of data protection.

Table 1 : Summary of the DPDP Act's Structure

Chapter	*Sections*	*Description*
Chapter 1	Section 1-3	Preliminary: The chapter gives an overview of the scope and definitions of the Act, which establishes the framework of the rest of the legislation.
Chapter 2	Section 4-10	Obligations of Data Fiduciary: This chapter provides the obligations of data fiduciaries (organizations that deal with personal data) and the rights of data subjects, the rights to access, correct, and delete data.
Chapter 3	Section 11-15	Rights and Duty of the Data Principal: Provides the rights and duties of the Data Principal including access to personal data, correction and redress of grievance.
Chapter 5	Section 18-26	Data Protection Board of India: Details the creation and operation of the Data Protection Board, and the powers and the responsibilities of the board.
Chapter 6	Section 27-28	Powers, Functions, and Procedure to be observed by the Board: This chapter stipulates the operations and roles of the Board.
Chapter 7	Section 29-32	Appearance and Alternative Dispute Resolution: The appellate procedure, the Appellate Tribunal and voluntary undertakings.
Chapter 8	Section 33-34	Penalties and Adjudication: A discussion on the penalties that an individual will get in case of non-compliance and how the amount of the penalty will be handled.
Chapter 9	Section 35-44	Miscellaneous: Provides provisions on the powers of the government, compatibility with other laws and the rule-making power.

The chapters give a smooth overview of the way in which personal information is accessed, collected, and the manner in which it is handled and stored in India and the responsibilities and obligations of the various stakeholders, among them data fiduciaries, the Data Protection Authority (DPAI) and the data subjects themselves. The important chapters and sections of the Act are summarized in a Table 1:

Key Substantive Provisions of the DPDP Act

Preliminary Provisions (Sections 1–3)

The chapter establishes definitions of the title, scope and commencement of DPDP Act. It captures some important definitions like Personal Data, Data Fiduciary, and Data Principal and defines the applicability of the Act territorially. It is applicable to the personal information that is worked with in India, and to the foreign organization that sells goods/ services to the Indian residents. On the basis of this chapter, the whole law system is established.

Obligations of Data Fiduciaries (Sections 4–10)

This chapter provides the duties of Data Fiduciaries (processing personal data entities). It obliges them to process data in a lawful, transparent and with a given purpose. Data Fiduciaries must ensure data security, accuracy, and minimization. They must obtain informed consent from Data Principals and provide clear notices regarding data processing. Additionally, they are obligated to implement security safeguards and retain data only as necessary for the purpose it was collected.

Rights and Duties of Data Principals (Sections 11–15)

This chapter provides the definition of the rights of Data Principals- people, whose data is being processed. Such rights are the right to access, correct and delete their personal data. The Data Principals also have the option to revoke the consent and pursue remedy on grievances. It also defines their responsibility such as maintaining precision of the information given and avoiding impersonation. This chapter will allow Data Principals to have control over their data and hold Data Fiduciaries accountable.

Data Protection and Sanctions (Sections 16–17)

In this chapter, the author describes the circumstances in which the Central Government is able to control the transfer of data across borders. Section 16 gives the government the authority to

limit the transfer of personal information by Data Fiduciaries so that the data transfer is in compliance with the Indian standards of data protection. Section 17 outlines exemptions of certain stipulations in the Act, including legal roles, national security, law and order, financial requirements (e.g. defaults on loans) or government actions. It also enables data processing to be done so as to conduct research or statistical analysis and it also enables the Central Government to give temporary exemptions to certain Data Fiduciaries such as startups.

Data Protection Board of India (Sections 18–26)

The chapter sets up the Data Protection Board of India (DPBI) that is charged with the responsibility of monitoring adherence to the Act. The DPBI researches breach of data, imposes a fine, and acts as a body of adjudication to settle disputes between Data Principals and Data Fiduciaries. The chapter establishes the composition of the Board, appointment of its members, and its power to implement the provisions of the Act, which ensures the provision of effective protection of the personal data.

Powers, Functions, and Procedure of the Board (Sections 27–28)

The powers and working procedures of Data Protection Board are discussed in this chapter. It implicitly grants the Board the authority to probe the complaints, punishments, and corrective measures to non-compliance. The Board is as well mandated to give directions and makes sure that Data Fiduciaries abide by the requirements of the Act. It also details the procedure that the Board should adopt when dealing with complaints and enforcement decisions with a focus on efficiency and transparency.

Appeal and Alternate Dispute Resolution (Sections 29–32)

In this chapter, a process of appeals and alternative dispute resolution (ADR) is given. It also enables individuals or organizations to seek an appeal of the decisions of the Data Protection Board to the Appellate Tribunal. Mediation is another option that is presented in the chapter as a way of solving disputes. It enables the Board to receive voluntary commitments by parties thus enabling quicker and more productive resolution without the protracted legal case.

Penalties and Adjudication (Sections 33–34)

This chapter presents the fines of breaking the DPDP Act. It states that the sanctions will depend on the extent and the term of the violation, the kind of data, and corrective measures. The Board has the powers to give fines and such fines are charged to Consolidated Fund of India. Such a framework should prevent or prevent non-compliance and make sure that Data Fiduciaries are responsible with their actions.

Miscellaneous Provisions (Sections 35–44

This chapter has got several miscellaneous provisions, including the authority of the Central Government to provide rules, amendments, and notifications to implement the Act. It provides the congruence of the DPDP Act with the rest of the Indian laws, having a definite resolution to any legal conflict. It also describes the jurisdictional role of the Data Protection Board and affirms that the Board has the only power over the issues that fall within the scope of the Act.

Core Objectives and Operational Mechanisms of The DPDP Act

Consent Management

Informed consent is one of the major fundamental principles of the Digital Personal Data Protection Act, 2023 (DPDP Act). Since data privacy has become a significant global issue, the Act provides clear guidelines on how consent is obtained and used. The DPDP Act (Section 6)[18] requires that consent be freely given, specified, communicated, and clearly expressed by individuals. According to the law, the data subject must have clear information about how, when, and why their data is processed. Moreover, Section 6 states that consent must be revocable at any time, allowing people to control their personal data throughout its lifecycle. This revocability ensures the system's dynamism and flexibility, allowing data subjects to exercise their rights as circumstances change, thereby fostering

user autonomy over their personal information. These conform to the international best practices, such as the requirements of the General Data Protection Regulation (GDPR), which also regards informed, granular consent as a basis of a lawful data processing. However, the DPDP Act puts a lot of attentiveness to the realities of consent withdrawal, since it allows the users a ready option to withdraw the consent to collection of their data without incurring any consequences.[19]

Rights of Data Subjects

The DPDP Act provides data subjects with immense rights to determine the way they capture, process, and share their data. Section 12-15 gave a statement of some of the most significant rights, including:

Right to access

The subjects of personal data have the right to access their own personal data collected by a data fiduciary in an easily readable and understandable form in a manner that they can verify authenticity and veracity of the data-gathering process.[20]

Right to Correction

The data subjects are entitled to correction of data kept about them in the event of inaccuracy or incompleteness of information presented by the respective organizations that represent them.[21]

Right to Erasure (Right to be Forgotten)

According to the provision, the data subject is entitled to demand that his/her personal data be erased in case it is not necessary anymore to fulfill the purposes, it was initially gathered, or because the subject has withdrawn his/her consent.[22]

Right to Data Portability

This enables individuals to receive their own personal information in one digital economy company and transfer it to another, in turn increasing market competition and offering customers a wider choice. This right is synonymous with the provisions of GDPR, but due to the differences in the data storage and access in India, it is not easy to enforce.[23]

The rights are founded on the international standards of data protection but adjusted to the context of the laws, technologies, and cultural specifics of India. The DPDP Act provides an excellent pattern of protection, yet the effectiveness of these rights will be seen based on the enforcement processes and the willingness of the organizations to follow these values.

Obligations of Data Fiduciaries

The central concept in the DPDP Act is that of data fiduciaries, or those organizations or entities collecting, processing, or retaining personal data.[24] In *Section 4*[25] the responsibilities of data fiduciaries are explicitly set and they are expected to operate in good faith and in the best interests of data subjects. Such fiduciaries should take care to minimize data collection, ensuring they gather only as much data as is required to achieve the above-mentioned purpose. Moreover, data fiduciaries must provide transparent, easily readable privacy notices, maintain transparency in their data practices, and uphold strong security controls to prevent privacy violations involving personal data. These roles place a heavy burden on organizations to build trust with users, especially in a market increasingly sensitive to data abuse and security breaches. The DPDP Act is inspired by international regulations, including the GDPR, which hold data controllers and processors to higher standards of accountability and privacy-by-design.[26] The provisions of the Act are strict, but it is still unclear how effectively authorities will be able to implement them, given the difficulties with data regulation and the rather heterogeneous Indian business environment.

Mechanisms of Enforcement and Compliance

According to Section 18-20, the Data Protection Board of India (DPBI) is the central body in making sure that the DPDP Act is adhered to. The powers of DPBI are rather extensive and it might investigate complaints, audit and punish violations. The Act also has a way of appealing: the entities may appeal against the DPBI decisions to the Appellate Tribunal that provides the checks-and-balances mechanism. Non-compliance will lead to hefty fines, the amount of which is proportional to the extent of the violation. The intention behind these measures is to motivate organizations to implement

compliance strategies and invest in data protection infrastructure. The mandate of the DPBI is apparent; the success of these enforcement provisions, however, depends on its operational capacity, the extent of cooperation from data fiduciaries, and the speed at which complaints are resolved. The enforcement mechanism shall evaluate the practical effects of the DPDP Act. Provided that the DPBI will be in a position to enforce compliance and impose penalties for non-compliance, it may serve as a model for other jurisdictions. Conversely, incompetent enforcement systems can undermine the provisions of the Act.

Cross-Border Data Transfer

Transborder data transfer is one of the main points of the DPDP Act since India has an increased digital economy and is involved in the global tech industry. Section 16[27] gives the regulatory framework of transfer of personal data outside India. According to the Act, personal data can only be submitted to other countries where the country receiving the data has sufficient data protection mechanisms or when the Data Principal has approved the submission. Although India's data localization provisions have become more flexible over time, restrictions on cross-border data flows remain significant. These restrictions are primarily intended to protect national interests, though concerns arise regarding their potential impact on international businesses, particularly those operating globally. The DPDP Act shares similarities with the GDPR by requiring organizations to ensure data protection for data transferred outside India, as the GDPR mandates the safeguarding of EU data in compliance with EU standards. However, in India, the challenge lies in balancing facilitating global data flows with enforcing domestic data protection regulations, especially as international companies expand into the Indian digital market. The DPDP Act will have a major impact on the future of data privacy in India as it progresses to become digital. The interpretation of these provisions is crucial to the measurement of the Act and its success in promoting the security and innovative digital economy and safeguarding human rights.

Criticisms And Challenges

Scope and Limitations

The biggest flaw of the Digital Personal Data Protection Act, 2023 (DPDP Act) is that it exempts the government especially when it comes to national security and law and order. The Act also allows government agencies to process personal data under section 17[28] without many restrictions, thereby bypassing most of the precautions that apply to fiduciaries of personal data. Although some may justify such exemptions in certain instances, critics argue that government agencies might use them to justify unchecked monitoring or mass-scale data collection, thereby compromising the Act's intent (Bisht & Sreenivasulu, 2024). Such a division of rights, in which individuals hold rights and the government has flexibility, can create an unequal situation that undermines overall personal data protection. The DPDP Act has been criticized for its limited scope in protecting personal data and for failing to consider a broader privacy and security perspective. The Act is mainly concerned with data in the control of data fiduciary, but this does not include any detailed provisions to acknowledge the increasing use of non-personal data and metadata. Such a limited approach may leave big gaps in protecting individuals against new types of data abuse, such as those facilitated by artificial intelligence (AI), big data analytics, and automated systems of decision-making. The increased topicality of these technologies demands the expansion of the data protection legislation and the revision of the new types of data usage and responsibility in automated procedures.

Enforcement Challenges

Although the sanctions for breaches under the DPDP Act, as outlined in Section 33[29], are intended to deter non-compliance, critics claim they are insufficient to induce significant compliance by large corporations. Since penalties are perceived as relatively low in organizations, they may be regarded as a cost of doing business rather than a deterrent. This issue is aggravated by the fact that authorities have not established clear guidelines for applying

such penalties, particularly in cases involving large-scale data breaches or the illegal release of sensitive information. To be truly effective, the penalties imposed by the Act must be meaningful enough to compel compliance but not so substantial as to deter data fiduciaries from strengthening their data protection mechanisms. In addition, enforcing the Act's provisions is very challenging. Although larger companies are likely to be able to afford the resources needed to comply with the DPDP Act, small enterprises and startups may not be able to meet its strict compliance requirements. For most of these entities, compliance costs such as legal advice, infrastructure upgrades, and employee training may be prohibitively expensive. This fact raises the question of whether the Act is reasonable in creating a level playing field where every player is obligated to adopt the same high standards of data protection, whether it is a large or a small entity.

Impact on Innovation

The potential impact on innovation, particularly in artificial intelligence (AI), is one reason the DPDP Act should be viewed as a more worrisome piece of legislation.[30] The current framework of the Act may impose heavy restrictions on AI systems that cannot operate efficiently without large amounts of personal data. As AI becomes increasingly apparent and tangible across the healthcare, financial, and marketing industries, the DPDP Act's ban on data use might be a limiting factor for organizations developing innovative technologies or data-driven solutions.[31] The compliance expenses of AI among startups and SMEs can affect their development or entry into the market without being intended because these companies might not fit into the laws of data protection and the moral principles that the AI systems have to meet.

On the contrary, such problems have also started to be discussed by the General Data Protection Regulation (GDPR) of the European Union. It has certain provisions to promote ethical uses of AI and protect fairness of inherent decision-making.[32] The GDPR imposes strict limits on automated profiling and requires individuals to be notified when they are processed solely by algorithms, thereby permitting them to challenge any decision.[33] All these actions are aimed at ensuring that AI creators apply the technology ethically and, at the same time, enabling innovation, which serves as a significant precedent for India. Unfortunately, the DPDP Act does not provide explicit guidelines on how AI systems are to operate within data protection law, leaving the possibility of misuse or unethical practices by data fiduciaries seeking to exploit AI to process data.

Data Localization and Cross-Border Data Transfer

The other concern is the localization of the data requirement which was defined by the DPDP Act. Section 16[34] also mandates that some kind of personal data are stored in India and this puts into question the operations of global businesses in India. Multinational companies may find it expensive to maintain data systems globally since data localization demands may be expensive. There is a criticism that such restrictions would impede free movement of data across borders and hence undermine the development of the digital economy in India and make the operations of Indian businesses difficult into the global markets. Though local storage of data may have certain security benefits, the benefits may restrict the interoperability of data across the world and their applicability in the digital supply chain.

The issues connected to AI and deepfakes, particularly the lack of specific regulation of such technologies, must be incorporated into the discussion of challenges regarding the Impact on Innovation.[35] In this section, the author will underscore that the DPDP Act is also not well-suited to address AI technologies and automated systems, which may pose risks due to misuse and ethical issues. Moreover, the report may note that the absence of clear rules governing the use of AI-generated content and deepfake technologies creates Enforcement Challenges.

Comparative Perspective: EU and US Regulations

In order to see the impact of these issues on the digital economy of India, it is worth discussing the DPDP Act in conjunction with EU and US legislation, which has a different approach to data protection.

The GDPR is an elaborate law regarding data protection and prioritizes the rights of data subjects and the ethical application of AI. Unlike the DPDP Act, the GDPR gives a clear stipulation to organizations to be more transparent about the application of AI and other automated decision making systems in such a way that these systems do not oppress the ethical framework.[36] The US, conversely, adopts a more sectoral policy with regulations like CCPA and HIPAA that apply to the protection of data in particular industries, providing a low level of unity and consistency within the digital space.[37]

Although the DPDP Act offers an in-depth approach to data protection, it has significant problems, especially regarding its impact on AI innovation and the lack of explicit ethical standards for its use.[38] The international contrast between the GDPR and US rules points to the need for more specific clauses to regulate new technologies.[39] The paper will identify key gaps in the DPDP Act and propose amendments to ensure that India's data protection law fosters innovation without jeopardizing privacy or the ethical application of new technologies, including AI. Whether data privacy in India can be achieved will depend on how the DPDP Act keeps pace with these evolving technological challenges.

Recommendations For Reform

The Digital Personal Data Protection Act, 2023 (DPDP Act) can be described as an important move in enhancing data privacy in India. But there are minor details which should be narrowed down to cover emerging technology challenges.[40] he development of artificial intelligence (AI), deepfakes, and generative AI-based applications (social media platforms, e.g., ChatGPT and Google Gemini) are new privacy issues that were not well tackled by the Act.[41]

Strengthening the Data Protection Framework

Expanded Definitions of Sensitive Data

The Act should broaden its definitions to include AI-generated, biometric, and genetic data, ensuring all sensitive categories are fully covered.

Regulation of Emerging Technologies

Regulators need to develop clear policies for AI and blockchain technologies, especially regarding automated decision-making and data processing. They must control AI-generated content, including deepfake videos and automated social media posts, to prevent its abuse, identity theft, and privacy invasions.

Data Portability & Right to be forgotten

Data portability and the right to be forgotten. The legislators should also consider having stronger data portability and right-to-be-forget legislation that allows a person to gain control over their information, particularly within the cloud storage and social media era.

Enhancing Enforcement and Penalty Regime

Strengthening Punitive Measures

It is necessary to make the punishments for violations and data breaches more explicit and severe to serve as a strong deterrent. They are supposed to correlate the financial fines to the magnitude of non-compliance.

Establishment of a Dedicated Cyber Tribunal

The government should establish a cyber tribunal, such as the Cyber Appellate Tribunal (CAT), to handle data privacy breaches, ensuring quicker resolutions and greater accountability for data protection issues.

Ensuring Independent Regulatory Oversight

Strengthening the Independence of the DPAI

The Data Protection Authority of India (DPAI) should not be dependent on the government to operate with a clear mandate from the people. The government should provide the DPAI with the resources necessary to maintain control over different sectors and to engage in compliance monitoring.

Global Harmonization of Data Protection Standards

International Standards

The DPDP Act should meet the international data protection requirements, especially the General Data Protection Regulation (GDPR) so that international data transfer can be facilitated, consistency in data protection laws, as well as to allow Indian businesses to act in accordance with the global data protection regulations.

Regulating AI, Deepfakes, and Generative AI

Ethical Use of Artificial Intelligence

The DPDP Act does not have any specific rules on AI-generated content, such as deepfakes or generative AI systems like ChatGPT. Such technologies can misrepresent, divide opinions, and invade the privacy of individuals or organizations.

Regulation of Deepfake Technologies

The Act should establish the regulation of the deepfake technology and the responsibility of AI-created materials. The lawmakers must come up with clear and ethical rules upon how AI can be used, and especially the rules about impartiality and responsibility.

Establishing an Ethical AI Framework

The Act ought to set the ethical uses of AI in content creation, which will include abuse that will mislead or invade privacy.

The above recommendations are meant to enhance the DPDP Act by making it adaptable to meet the needs of the AI technologies, deepfakes, and new platforms. As this is expanded to cover such technologies and more narrow application controls, India may be able to become the global leader on the privacy of data, not implying that it should cease technological advancement. The future of data protection in India will depend on whether the DPDP Act will be modified to these new technological changes, and keep ensuring the privacy of people without suffocation of development.

Case Law Analysis

Puttaswamy v. Union of India (2017)

- ***Right to privacy***

According to the Indian constitution, the Supreme Court has identified the right to privacy as being a fundamental right in Article 21.

- ***Impact on the DPDP Act***

The ruling formed the foundation of the Digital Personal Data Protection Act, 2023 (DPDP Act) that deals with such aspects as informed consent, the rights of the data subjects, and the rights to access, correct, and erase information.

- ***Proportionality Test***

The government emphasized the proportionality test in state actions that affect privacy. The DPDP Act includes provisions that allow it to grant exemptions for national security or the common good, but these exemptions are subject to scrutiny to prevent overreach.

Individual Autonomy

The ruling affirmed the importance of personal autonomy on the internet, one of the DPDP Act's main pillars.

Shreya Singhal v. Union of India (2015)

Freedom of Expression

The Supreme Court struck down Article 66A of Information Technology Act, 2000 claiming that it amounted to violation of freedom of speech, as enshrined in Article 19(1) (a) of the Constitution.

Privacy and Free Speech

This case influenced the DPDP Act, which does not limit privacy rights in the name of freedom of speech. The Act provides explicit direction to data fiduciaries, establishing a balance between privacy and personal rights to express themselves freely.

Regulatory Clarity

The case has shown the need for greater clarity in the regulatory framework governing online content.

The DPDP Act will support this by providing data fiduciaries with a transparent structure that makes data practices transparent without limiting speech.

The Puttaswamy and Shreya Singhal decisions have influenced India's data protection legislation by affirming the inherent right to privacy and the necessity of specific, balanced regulation in the digital world. These principles are combined in the DPDP Act, and it is reasonable to believe that it adheres to the rights enshrined in the Constitution, even though it provides a clear and moral framework for managing data. The analysis of the impact of such cases helps determine whether the DPDP Act is consistent with constitutional values and responsive to the new challenges of digitality.

Conclusion

This paper has undertaken a critical analysis of the Digital Personal Data Protection Act, 2023 (DPDP Act). It compared its key provisions and issues with how it has encountered challenges especially with the introduction of new technologies especially artificial intelligence (AI) and deep fake technologies. On the basis of the analysis of the DPDP Act in correlation with the key case law and international standards, the given research shows the vulnerability of the current system designed to safeguard the data of Indians. The most interesting finding of the research is that the Act possesses a strong foundation of privacy protection due to such landmark cases as Puttaswamy and Shreya Singhal. These are few examples which helped in shaping the DPDP Act in line with the fundamental rights, most notably the right to privacy and the expression of freedom of speech. Among the gaps in the study, however, there are critical ones, in particular, in the control of emerging technologies, such as AI, deepfakes, and automated systems. The stillness of the Act in terms of providing a clear direction on how AI and deepfakes can be utilized morally is a major weakness and it provides the possibility of misuse in the cyber world. The study is innovative compared to past studies as it discusses AI and deepfake technologies that have not been examined in the current data protection legislation in India. Moreover, it also shows how stronger control means and more powerful penalties should be used to make sure that people comply and do not jeopardize data. Despite the fact that the DPDP Act is a great move in the right direction, future research ought to aim at creating more elaborate rules that will regulate AI, international data flows and data ethics. The impact of new technologies on information security needs close attention, and the flexible regulatory framework is needed to follow the field of technological advancement. In addition, enforcement mechanisms are very important in determining the success of the DPDP Act. These aspects will be strengthened to provide more efficient protection of the data and improved adaptation to changing technological environments.

References

Press Information Bureau. (2025, October 8). Curbing cyber frauds in Digital India. Government of India. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3

Malhotra, C., & Malhotra, U. (2024). Putting interests of digital nagriks first: digital personal data protection (dpdp) act 2023 of India. *Indian Journal of Public Administration*, *70*(3), 516-531.

Jain, A., & Anand, A. (2025). Tracing the Constitutional Journey of Data Privacy in India: From Puttaswamy to the Draft DPDP Rules, 2025. *Available at SSRN 5283949*.

Ahmed, S., & Nasir, M. Digital Personal Data Protection Act, 2023: A Critical Analysis. *INDIAN STUDIES REVIEW*, 1.

Gomes, S. M. P. J. (2024). *EU Personal Data Protection Standards Beyond Its Borders: An Analysis of the European External Governance Through GDPR on Data Protection Laws in the ASEAN Region* (Master›s thesis, ISCTE-Instituto Universitario de Lisboa (Portugal)).

*Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors.***,** (2017) 10 SCC 1**.**

Sharma, D., & Choudhury, S. The Right to Privacy in the Era of Digitalization: Legal Challenges and Solutions.

Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

Abbas, K. (2023). Navigating the Digital Maze: Freedom of Expression in India's Digital Democracy. *Part 2 Indian J. Integrated Rsch. L.*, *3*, 1.

Bharanitharan, K., & Kaur, G. (2024, October). A Comparative Analysis of Data Minimization Principles: Evaluating GDPR and India's DPDP Act 2023. In *International Conference On Data Mining And Information Security* (pp. 41-55). Singapore: Springer Nature Singapore.

Fakeyede, O. G., Okeleke, P. A., Hassan, A., Iwuanyanwu, U., Adaramodu, O. R., & Oyewole, O. O. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *International Journal of Research in Engineer-*

ing and Science, *11*(11), 45-58.

Id.

Iman, N. (2024). The fight for our personal data: analyzing the economics of data and privacy on digital platforms. *International Journal of Law and Management*, *66*(6), 774-791.

Kumar, A. (2019). The Right To Be Forgotten in Digital Age: A Comparative Study of the Indian Personal Data Protection Bill, 2018 & the GDPR. *Shimla Law Review*, *2*.

Kaur, N. (2025). Decoding the Digital Personal Data Protection Bill: Strengths, Weaknesses, and the Road Ahead. *Weaknesses, and the Road Ahead (January 04, 2025)*.

SWARGIARY, K. (2025). *A Comprehensive Study of Technology Law in India: Challenges, Compliance, and Future Directions*. GOOGLE.

A&O Shearman on Data. (2023, August 18). India – Digital Personal Data Protection Act receives Presidential assent. Retrieved from https://www.aoshearman.com/en/insights/ao-shearman-on-data/india--digital-personaldata-protection-act-receives-presidential-assent

The Digital Personal Data Protection Act, 2023, Sec. 6.

Jain, A. S. (2025). Decoding consent managers under the Digital Personal Data Protection Act, 2023: Empowerment architecture, business models and incentive alignment. *Journal of Data Protection & Privacy*, *7*(4), 406-420.

Panchal, S. (2024). Cross-Border Data Protection Laws in India and European Union: A Critical Analysis of the Complexities and the Legal Challenges.

Bansal, A., & Goyal, G. (2025). Digital Personnel Data Protection Act: A Survey. *Available at SSRN 5285948*.

Sharma, S., & Kasat, M. (2024). Right to Be Forgotten: An Indian Perspective. *Issue 1 Int'l JL Mgmt. & Human.*, *7*, 597.

David, Y. (2023). Legal Implications of Data Monetization by Commercial Entities. *Available at SSRN 4922310*.

Collaco, A. M. (2025). Contours of data protection in India: the consent dilemma. *International Review of Law, Computers & Technology*, *39*(2), 194-212.

The Digital Personal Data Protection Act, 2023, Sec. 4.

Chaudhary, V. K., & Verma, D. (2025). THE NEW FRONTIER OF DATA PROTECTION: UNDERSTANDING INDIA'S DPDP RULES AND GLOBAL COMPLIANCE. *PANJAB UNIVERSITY LAW MAGAZINE-MAGLAW*, *4*(1).

The Digital Personal Data Protection Act, 2023, Sec. 16.

The Digital Personal Data Protection Act, 2023, Sec. 17.

The Digital Personal Data Protection Act, 2023, Sec. 33.

Usha, T., & Neeral, G. (2025). Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023. *Legal Issues in the digital Age*, (2), 87-117.

Iyer, S. S. (2025). Data-Driven Decision Making: The Key to Future Health Care Business Success.

Sartor, G., & Lagioia, F. (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence.

Hänold, S. (2018). Profiling and automated decision-making: Legal implications and shortcomings. In *Robotics, AI and the Future of Law* (pp. 123-153). Singapore: Springer Singapore.

The Digital Personal Data Protection Act, 2023, Sec. 16.

Alanazi, S., Asif, S., Caird-daley, A., & Moulitsas, I. (2025). Unmasking deepfakes: a multidisciplinary examination of social impacts and regulatory responses. *Human-Intelligent Systems Integration*, 1-23.

Ogobegwu, J. N. (2024). *General Data Protection Regulation (GDPR) and its Impact on the Development of Artificial Intelligence (AI) in Marketing* (Master›s thesis, ISCTE-Instituto Universitario de Lisboa (Portugal)).

Hawamdeh, S. S. (2025). Cybersecurity and Data Privacy Laws: Balancing Innovation and Protection in the Digital Age. *Middle East Journal of Economics, Law and Social Sciences (MEJELSS)*, 36-46.

Usha, T., & Neeral, G. (2025). Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023. *Legal Issues in the digital Age*, (2), 87-117.

Bakare[1], S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh[4], N. E. (2024). Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations.

Dave, A., & Agrawal, A. K. (2025, May). A Comparative Study with GDPR, HIPAA, CCPA, PIPEDA and DPDPA. In *2025 IEEE International Conference on Computer, Electronics, Electrical Engineering & their Applications (IC2E3)* (pp. 1-6). IEEE.

Islam, T. (2024). *Regulatory challenges of AI governance in the era of CHATGPT*. Kluwer Law International BV.