INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 4 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 4 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-4-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 4 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

BALANCING AI INNOVATIONS WITH PRIVACY LAWS (IN LIGHT OF INDIA'S DPDP ACT, 2023)

AUTHOR – PARAS SHARMA* & BHAVYA SHARMA**

* STUDENT AT AMITY LAW SCHOOL, NOIDA

** MENTOR AT AMITY LAW SCHOOL, NOIDA

BEST CITATION - PARAS SHARMA & BHAVYA SHARMA, BALANCING AI INNOVATIONS WITH PRIVACY LAWS (IN LIGHT OF INDIA'S DPDP ACT, 2023), *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (4) OF 2025, PG. 1130-1142, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

This article explores the balance between AI innovation and privacy protection in the digital era, focusing on India's Digital Personal Data Protection (DPDP) Act, 2023. The Act represents a significant effort to regulate how personal data is collected, stored, and used, ensuring that individual rights are safeguarded. However, as AI technologies continue to evolve, new challenges emerge that the current framework does not fully address. This article reviews the key provisions of the DPDP Act, examines its practical implications for data fiduciaries and individuals, and highlights areas where further reforms are needed. The article provides clear recommendations for improving the legal framework so that it both promotes progress and protects fundamental privacy rights.

Introduction

Artificial intelligence is pushing the limits of innovations that were once unimaginable. From being able to solve simple math problems to offering personalized healthcare tailored to unique symptoms and conditions of patients. AI has come far and we have witnessed it grow, we have seen its limitless potential. While innovation drives technological progress, it must coexist with legal frameworks designed to protect individual rights. The intersection of artificial intelligence and privacy laws is one of the most pressing challenges of our time. This rapid advancement raises significant concerns. As AI systems become more powerful, their ability to process vast amounts of personal data raises critical questions about security, consent, and ethical responsibility. This article explores how AI innovation and privacy laws interact, sometimes in conflict and sometimes in harmony in light of India's Digital Personal Data Protection Act, 2023.

What is AI?

Artificial Intelligence or AI is a technology that allows computers to perform tasks that typically require human intelligence, such as learning, understanding, and making decisions. AI requires quite vast amounts of data to reach an operational point. There are branches of AI which are concerned with trying to imitate human behaviour, i.e. learning, observing, understanding and then making decisions based on those. These branches are mainly machine learning and deep learning.

1. Machine Learning: This is a branch of AI that uses algorithms that enable computers to learn and recognise patterns from data and make decisions without being explicitly programmed to. Instead of following a set of rules, these AI models improve over time as they process more data.

a. Applications:

i. Recommendations: Netflix, YouTube and Spotify suggest movies, videos, music and songs based on user behaviour.

ii. Spam Filter: Email services use machine learning to filter out spam and phishing emails.

iii. Fraud Detection[1809]: Banks and financial institutions use machine learning to detect fraudulent transactions.

iv. AI assistants: Google Assistant, Siri, Alexa, Rufus, Gemini etc… use machine learning to provide relevant answers to your queries.

v. Self Driving cars: Tesla and other companies use machine learning to recognize objects, predict movement, and make driving decisions.

2. Deep Learning: This branch of AI is a more advanced subset of machine learning that uses neural network matrices to analyse complex data and make highly accurate predictions.

a. Neural Network: Inspired by the human Brain, it involves networks of algorithms which have multiple layers (hence "deep") and are thus capable of processing, analysing more complex data.

b. Applications:

i. Facial Recognition: Used in smartphones(Face ID), security systems, airports, and social media tagging.

ii. Medical Diagnosis: AI model can scan MRI, CT scans and X-rays to detect diseases.

iii. Autonomous Vehicles: Deep learning helps self-driving cars process real-time data from cameras and sensors.

iv. Natural Language Processing (NLP): AI models like ChatGPT, Google Translate, and Grammarly understand and generate human-like text.

v. Deepfake Technology: AI can generate realistic human faces and modify videos, often used for entertainment or misinformation.

In short, Machine Learning is effective for structured data like numbers, tables, and simple classification tasks.

Deep Learning excels at handling large, unstructured data like images, videos, and speech.

AI's Journey

First mention of AI can be traced back to 1946 when English Computer Scientist Alan Turing coined the term "Artificial Intelligence". AI's first revelation was done in the 1950s when British Computer Scientist Christopher Strachey, wrote a program that successfully ran Checkers. Then in the 1990s, IBM's Deep Blue beat the then Grandmaster Garry Kasparov. AI evolved from a simple system that operated on "if/then" rules that couldn't adapt to new situations beyond programmed rules to an advanced system that can mimic the Human Brain.

How AI is Driving Innovation Across Industries

AI is transforming industries by automating tasks, improving efficiency, and unlocking new possibilities.

- Healthcare: AI is revolutionizing healthcare by enhancing diagnostics, personalizing treatments, and accelerating drug discovery. AI-powered radiology systems analyze medical images such as X-rays, MRIs, and CT scans with remarkable accuracy, assisting doctors in detecting diseases like cancer at an early stage. Personalized treatment plans are another breakthrough, where AI analyzes a patient's medical history and genetic data to recommend tailored treatment, as seen in AI-driven oncology solutions like IBM Watson. Additionally, AI is significantly reducing drug discovery timelines by predicting molecular interactions, helping pharmaceutical companies develop new medicines faster, as demonstrated by AI-driven drug research from DeepMind and Moderna. These advancements lead to more efficient healthcare, improved patient outcomes, and reduced costs.

[1809] https://www.outsystems.com/ai/machine-learning-overview/

- Finance: In the financial sector, AI plays a critical role in fraud detection, automated trading, and risk assessment. Banks and financial institutions leverage AI to monitor transactions in real-time, identifying suspicious activities and preventing fraudulent transactions with advanced anomaly detection techniques. AI-driven algorithms also dominate high-frequency trading, executing trades at optimal times based on market trends, maximizing profits while minimizing risk. Moreover, AI enhances risk management by analyzing vast datasets to determine creditworthiness and potential financial risks, as seen in AI-powered credit scoring systems like those used by ZestFinance. By integrating AI, financial institutions achieve increased security, efficiency, and better decision-making.

- Retail & E-Commerce: AI has transformed retail and e-commerce by enhancing customer experiences and optimizing sales strategies. Chatbots and virtual assistants provide instant customer support, handling queries and guiding users through shopping platforms. Recommendation engines analyze user behavior and purchase history to suggest relevant products, significantly improving engagement and sales, as seen on platforms like Amazon and Netflix. Additionally, AI enables dynamic pricing, where algorithms adjust prices in real-time based on demand, competitor pricing, and customer behavior, a strategy commonly used by airlines and ride-hailing services like Uber. Through AI-driven personalization and automation, businesses can increase customer satisfaction and revenue.

- Transportation: The transportation industry is undergoing a major shift with AI-driven innovations like autonomous vehicles and intelligent traffic management systems. Self-driving cars, powered by deep learning and computer vision, can recognize objects, predict movements, and make split-second driving decisions, as demonstrated by Tesla's Autopilot and Waymo's autonomous taxis. Meanwhile, AI-based traffic management systems analyze real-time data from cameras and sensors to optimize traffic flow, reduce congestion, and improve road safety in smart cities like Singapore. These advancements are paving the way for safer, more efficient, and sustainable transportation systems.

- Manufacturing: AI is reshaping manufacturing through automation, predictive maintenance, and supply chain optimization. AI-powered robots are widely used in assembly lines to handle repetitive tasks with precision, increasing productivity and reducing human errors, as seen in Tesla's automated car manufacturing process. Predictive maintenance, another key innovation, allows AI to analyze machine data and predict equipment failures before they occur, minimizing downtime and saving costs. Additionally, AI optimizes supply chain operations by predicting demand and managing inventory, a strategy effectively employed by Amazon's warehouses. These AI-driven solutions lead to more efficient and cost-effective manufacturing processes.

- Education: In education, AI is creating personalized and accessible learning experiences. AI tutors provide students with real-time assistance, adapting lessons based on their individual progress, as seen in platforms like Duolingo and Squirrel AI. Personalized learning systems analyze students' strengths and weaknesses, customizing educational content to maximize their understanding. AI is also being used to automate grading, reducing teachers' workloads by instantly assessing multiple-choice tests and, in some cases, even essays. By integrating AI into classrooms, education is becoming more inclusive, efficient, and tailored to individual learning needs.

Even governments use AI for development of Urban areas and in intelligence assistance. However, here's the catch, AI thrives on data, the more data it processes, the smarter and more accurate it becomes. AI's ability to analyze massive amounts of data and make real-time

decisions is revolutionizing these fields, but it's omnipresence raises serious questions:

1. Where does this data come from?
2. Who controls this data?

And when these questions are answered that is where the privacy concerns rise:

1. The data comes from Us, the Users of these AI services or in legal terms Data Principals.
2. Government and Regulatory bodies control a lot of personal data of citizens. Big corporations who operate these AI models use publicly available as well as User generated data.

AI is collecting our data constantly, ranging from search history and online purchases to behavioural data and audio-visual data. This raises some major ethical concerns:

1. Are we truly giving our informed consent for collection of our data?
2. Can AI be biased, leading to unfair decisions?
3. Are we being surveilled without our knowledge?

The DPDP act addresses some of these concerns.

India's Digital Personal Data Protection Act, 2023("**DPDP Act, 2023**")

The Digital Personal Data Protection act is India's first legal framework after the IT acts of 2000 designed to regulate collection, storage and processing of personal data while protecting individual rights. Although the act was passed by the Parliament on 9th August, 2023 and it received the assent of the president on 11th August, 2023, it is yet to be enforced as it is awaiting the approval and passing of Digital Personal Data Protection Rules, 2025, which is supplementary to its implementation. The act introduces strict data processing requirements, outlines the rights of the individuals, sets obligations for Data Fiduciaries(controllers), imposes restrictions on data transfer to other nations and levies penalties on those who violate the provisions of the act.

Data Processing and Requirements

- **Consent First approach(Section-6):**

Organizations must obtain free, specific, informed, unconditional and unambiguous user consent before collecting or processing data. Consent withdrawal must be allowed at any time.

- **Purpose limitations(Section-6):**

Data can only be processed for the stated purpose at the time of collection, ensuring that Data Fiduciaries do not misuse data beyond its intended scope.

- **Data Collection Specification(Section-6):**

AI models must only collect necessary data instead of indiscriminately gathering large datasets.

- **Use without Consent(Section-7, Section-11(2), Section-17):**

Certain exceptions exist where consent is not required, such as for government functions, legal obligations, or specific public interest purposes.

AI models that rely on large-scale personal data for training (e.g., recommendation engines, facial recognition, and predictive analytics) must now comply with stricter data collection limitations and consent mechanisms. Businesses using AI must ensure transparency in data usage.

Right of Individuals vs Obligations of Data Fiduciaries

The DPDP Act grants individuals (data principals) several rights while imposing strict obligations on organizations (data fiduciaries) that collect and process data. While these rights and obligations do not directly address the AI models, they do address the parent company or in this case Data Fiduciaries.

- Right of the Individuals(Section-11)

  - Right to access information about personal data:

    - Users can request access to their personal data and its summary that is being processed.

    - Users can request the identities of all other data fiduciaries that have access to their personal data via the principal Data Fiduciary including any personal data of such data principal and its processing.

  - Right to Correction or Erasure of personal data(Section12):

    - Individuals can request correction of incorrect data;

    - Completion of incomplete data;

    - Updating of outdated data;

    - Deletion of personal data when it is no longer needed or if consent is withdrawn.

  - Right to Grievance Redressal(Section-13):

    - Users must have a readily available way to raise complaints pertaining to exercise of rights of the Data Principal and performance of obligations of Data Fiduciaries.

  - Right to Nominate(Section-14):

    - Users must have the right to nominate any other individual, who can exercise the rights of data principal to their own personal data on their behalf in case of Death or Incapacity.

    - Incapacity is defined as inability to exercise the rights of data principal under the act.

AI companies must design user-friendly data management tools that allow individuals to exercise their rights easily, such as requesting data deletion or correcting AI-generated profiles.

- With Rights also come with Duties of Data Principal(Section-15):

  - Compliance with Lawful Obligations:

    - Data Principals must adhere to the provisions of the DPDP Act and other applicable laws while exercising their rights.

    - They cannot claim exemptions or rights under the Act if they engage in unlawful activities.

  - Respecting the Rights of Others Data Principals:

    - While individuals have data privacy rights, they must not use them to infringe upon the rights of others.

    - Eg, they cannot demand access to another person's personal data under false pretenses.(impersonation)

  - Providing Accurate Information:

    - Data Principals must ensure that the personal data they provide is accurate and up to date.

    - Misrepresentation or providing false information can lead to wrongful data processing and legal consequences.

  - Not Filing False or Frivolous Complaints:

    - Individuals must not misuse their rights under the Act by filing false, frivolous, or baseless complaints against Data Fiduciaries (organizations handling personal data).

    - This prevents unnecessary legal burden on businesses and the regulatory system.

The duties of Data Principals create a balance between privacy rights and accountability. While the DPDP Act empowers individuals with control over their data, these obligations ensure that rights are exercised responsibly and in good faith.

- Obligations of Data Fiduciaries(Section-8, 9, 10)

  - Lawful Processing & Consent:

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- Data must be processed only for lawful purposes, with clear user consent. Organizations should collect only the necessary data and use it only for the stated purpose.
- They, unless retention is necessary with any law in force at the time, delete the personal data in its entirety, once consent has been withdrawn. Ensure that the other data fiduciaries who accessed the Data from Primary fiduciary also delete the data.

○ Security and Safeguards:

- Data Fiduciaries must implement technical and organizational measures to prevent data breaches and unauthorized access.

○ Breach Notification:

- If a data breach occurs, fiduciaries must inform both the Data Protection Board and affected individuals.
- It does not matter how minor or major the leak is, whether a single individual was affected or numerous.

○ Appointing a Data Protection Officer (DPO):

- Appoint An in-country Data Protection Officer responsible for ensuring compliance and making sure that DPO's business contact information is available readily for Data Principle to contact.
- In case of readily available contact information, any person who speaks on behalf of the Data Fiduciary may also suffice, provided they can answer any questions raised by Data Principal about their personal data

○ Compliance with User Rights:

- Enabling User Rights:

- Companies must have accessible and effective complaint resolution systems for data privacy violations.
- Fiduciaries must allow users to access, correct, and delete their personal data upon request.

- Timely Response & Escalation:

- Organizations must respond to complaints within a reasonable timeframe, and unresolved disputes can be escalated to the Data Protection Board.

○ Protection of Personal Data of Children:

- India has one of the largest populations of underage internet users, making child data protection a crucial aspect of the DPDP Act.
- Parental Consent:

- Fiduciaries must obtain verifiable parental consent before processing any personal data of children (under 18 years).

- No Harmful Processing:

- Data processing that could cause harm to children's well-being, including tracking, profiling, or behavioral advertising, is strictly prohibited.

- Age-Gating Requirements:

- Platforms likely to be accessed by children must implement age-verification mechanisms to prevent unauthorized access to adult content or unsafe services.

Data Protection Board of India("**DPB**"):

○ Establishment, Composition and Status of the Board (Sections 18–19):

- The Act mandates that the Central Government, by notification, establishes the Data Protection Board of India.
- The Board is a corporate body with perpetual succession, property rights, and the authority to contract.
- The Board consists of a Chairperson and Members.(officers)
- The Board must conduct its meetings and transactions following prescribed procedures including digital meetings and proper authentication of its orders.
- It is empowered to appoint officers and employees (with Central Government approval) to ensure efficient functioning.

- All Chairperson, Members, officers, and employees are deemed public servants when executing duties under the Act.

○ Eligibility, Disqualifications (Sections 21–22):

- Individuals with integrity and specialized expertise in areas like data governance, law, ICT, or consumer protection are appointed as members with at least one legal expert.
- Members hold office for a two-year term which can be renewed and enjoy a prescribed salary and allowances that cannot be reduced post-appointment.
- Members face disqualification if they have issues such as insolvency, convictions involving moral turpitude, or conflicts of interest that might prejudice their functions.
- Removal from office is subject to a fair hearing, and any vacancies (due to resignation, removal, or death) must be filled by fresh appointments.

○ Powers of the Chairperson (Section–26):

- The Chairperson exercises general superintendence over all administrative matters of the Board.
- They may delegate tasks, scrutinize complaints and correspondence, and allocate proceedings among Members.

○ Powers of the Board (Section 27–28):

- The Board is empowered to direct urgent remedial or mitigation measures upon receiving a personal data breach notification, investigate complaints from Data Principals, and impose penalties as per the Act.
- It can issue directions after affording the concerned person an opportunity to be heard, and it holds powers similar to those of a civil court (e.g., summoning witnesses, receiving evidence, inspecting documents).
- Functioning as an independent digital office, the Board is designed to handle complaint receipt, allocation, hearings, and decision pronouncements digitally.
- It determines whether there are sufficient grounds to proceed with an inquiry; if not, it can close proceedings with reasons recorded, or if yes, it conducts a full inquiry following principles of natural justice.

○ Appellate Tribunal, ADR and Voluntary Undertaking(Sections 29–32):

- Any person aggrieved by an order or decision of the Data Protection Board can appeal to the Appellate Tribunal within 60 days of receiving the order. However, the Tribunal may allow a late appeal if it is satisfied that there was a valid reason for the delay.
- The Tribunal, after hearing both parties, may confirm, modify, or set aside the Board's decision and it must try to resolve the appeal within six months. If it takes longer, it must provide reasons in writing.
- The Tribunal is designed to function digitally, meaning appeals, hearings, and decisions should be processed online following the procedures specified under the Telecom Regulatory Authority of India Act, 1997, including provisions for further appeal to higher courts.
- The orders of the Appellate Tribunal are enforceable like a decree of a civil court provided it has all the powers of a civil court for execution.
- The Tribunal may send its orders to a local civil court, which will execute them as if they were its own decree.
- If the Data Protection Board believes a complaint can be resolved through mediation, it may direct the parties to attempt settlement.
- The Board can accept a voluntary undertaking from a person which may include commitments like taking corrective actions or refraining from certain actions.
- The Board, with the consent of the person, can modify the terms of the undertaking.

■ Once accepted, the undertaking prevents further proceedings on the same matter unless the person violates its terms but, If there is a breach of the undertaking, it is treated as a violation of the Act, and the Board may impose penalties.

○ Penalties(Section-33 and Schedule)[1810]:

■ If the Data Protection Board determines that a person/entity has significantly breached the provisions of the Act, it can impose a monetary penalty, but the board considers certain factors to decide the penalty amount:

- Nature, gravity, and duration of the breach.
- Type and sensitivity of personal data affected.
- Whether the breach was repeated.
- Whether the person gained financially or avoided loss due to the breach.
- Whether timely and effective action was taken to mitigate damage.
- The penalty should be proportionate and effective to deter future breaches.
- The likely impact of the penalty on the person.

■ The Schedule under Section 33(1) outlines the maximum monetary penalties for various breaches under the act:

- For failure of a Data Fiduciary to implement reasonable security safeguards to prevent personal data breaches (Section 8(5)) upto ₹250 crore.
- For failure to notify the Data Protection Board or affected individuals about a personal data breach (Section 8(6)) upto ₹200 crore.
- For breach of obligations related to children's data protection (Section 9) upto ₹200 crore.
- For failure to comply with additional obligations for Significant Data Fiduciaries (Section 10) upto ₹150 crore.
- For breach of Data Principal's duties (e.g., filing false complaints, misusing rights) (Section 15) upto₹10,000
- For breach of a voluntary undertaking accepted by the Data Protection Board (Section 32) upto Penalty up to the amount applicable for the related violation
- For any other violation of the Act or its rules upto ₹50 crore.

■ Miscellaneous(Section-35-44)

- Government & Board Members are shielded from liability if they act in good faith.
- The Government can demand data and block businesses that repeatedly violate data laws.
- The DPDP Act overrides conflicting laws but does not replace them entirely.
- Stronger restrictions on personal data disclosure under RTI, limiting transparency.
- Penalty limits can be revised, but not beyond 2 times the original maximum limit.
- Section 43A of the IT Act is removed, shifting all personal data protection to the DPDP Act. Section 81 is amended to ensure the DPDP Act prevails over conflicting provisions in the IT Act.

How AI and New Privacy laws Interact(AI innovations vs DPDP Act)

Artificial Intelligence has seamlessly integrated into our daily lives, influencing everything from personalized recommendations and financial decisions to healthcare diagnostics and automated hiring. As AI continues to evolve, its deeper incorporation across industries is inevitable. However, this rapid expansion raises significant concerns about data privacy, automated decision-making, profiling, and bias.

The Digital Personal Data Protection (DPDP) Act, 2023, serves as India's first comprehensive

[1810] https://www.medianama.com/2022/11/223-dpdb-2022-role-of-data-protection-board/

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

framework to regulate the processing of personal data, ensuring that AI-driven innovations operate within the bounds of privacy, security, and accountability. While the Act establishes strong protections for data collection, consent, and security, it lacks explicit AI governance provisions, leaving gaps in areas like automated decision-making, AI bias, and transparency.

What the DPDP Act can cover:

- Processes digital personal data (Section 3) – If an AI system processes personal data in digital form, whether inside or outside India, and offers services to individuals in India, the Act applies.
- Acts as a Data Fiduciary or Data Processor (Section 2) – Any entity that determines the purpose of processing personal data is a Data Fiduciary, while those processing data on behalf of another are Data Processors.
- Uses automated decision-making that affects individuals (Section 8(3)(a)) – AI-driven profiling, recommendations, or automated hiring decisions must ensure accuracy, consistency, and completeness of the data used.

Certain Key Provisions applicable to AI models:

- AI models must collect and process data only for a lawful purpose.
- Consent must be specific, informed, and explicit for AI-driven data usage (Section 6).
- If an AI system collects data for training purposes, it must disclose the purpose upfront (Section 5).
- If personal data was collected before the Act's enforcement, the Data Fiduciary must inform individuals and allow them to withdraw consent (Section 5(2)).
- No blanket consent for multiple unspecified uses – AI developers cannot collect data and later decide to use it for different purposes.
- AI systems cannot store personal data indefinitely – once the purpose is served, it must be erased.
- If an individual withdraws consent, the AI system must delete their data unless retention is required by law.
- Obligation extends to third-party AI models trained using that data
- AI models must ensure data accuracy if used to make decisions that affect individuals.
- AI-generated inferences are not exempt – if an AI system uses incorrect or biased personal data, the Data Fiduciary is accountable.
- No regulatory exemption for AI-generated decisions – meaning companies deploying AI-driven credit scoring, job filtering, or surveillance systems are liable for faulty AI outcomes.
- AI models must obtain verifiable parental consent before processing children's personal data.
- No profiling, tracking, or targeted advertising is allowed for minors.
- No exceptions – unlike GDPR, the DPDP Act does not provide a research exemption for AI innovation in child data processing.

If an AI company processes large-scale, sensitive, or high-risk data, the government may designate it as a Significant Data Fiduciary (SDF). This triggers additional obligations:

- Mandatory appointment of a Data Protection Officer (DPO).
- Regular Data Protection Impact Assessments (DPIA) to evaluate AI risks.
- External audits to assess compliance with the Act.
- No exceptions for AI startups – if an AI company meets the threshold, it must comply.
- If an AI system fails to secure personal data, it can face penalties up to ₹250 crore (Section 8(5)).

- If an AI firm fails to report a data breach, it faces a ₹200 crore fine (Section 8(6)).
- AI firms must have grievance redressal mechanisms – individuals can file complaints if their data is misused (Section 13).
- The Data Protection Board can investigate AI systems, issue compliance orders, and impose fines (Sections 27-28).

How Does this Affect AI Innovations:

- AI models trained on private personal data need explicit consent.
- Data minimization required – AI models cannot collect unnecessary personal data.
- Synthetic and anonymized datasets are safe – The Act does not regulate non-personal data.
- AI systems offering personalized services need user consent (e.g., recommendation engines).
- If AI models make automated decisions, users must be able to correct or challenge errors.
- Failure to protect user data leads to massive fines.
- Strict restrictions on child data usage – AI researchers cannot profile or track minors.
- No exemptions for AI research involving personal data – unlike GDPR, India's law does not exempt research purposes from data protection rules.
- No restrictions on AI research using synthetic or anonymized data.

Criticism

While the Digital Personal Data Protection (DPDP) Act, 2023 is a landmark legislation that establishes a legal framework for personal data protection in India, it has several gaps and shortcomings.

1. Problem: The DPDP Act does not address AI-driven automated decision-making, bias, or transparency.

a. Why it Matters:
AI systems process vast amounts of personal data, often making opaque, high-stakes decisions (e.g., credit scores, hiring, law enforcement).
Unlike GDPR (EU), the DPDP Act does not mandate AI explainability or fairness audits.

b. Solution: Introduce specific obligations for AI systems handling personal data, including right to explanation, human oversight, and bias audits.

2. Problem: The Data Protection Board of India (DPBI) is not truly independent, as its members are appointed by the Central Government (Sections 18-19).

a. Why it Matters:
The government has unchecked power over DPBI, raising concerns about political influence and selective enforcement.
Unlike GDPR, which establishes independent regulators, DPBI's autonomy is not guaranteed.

b. Solution: Ensure the DPBI operates independently, with fixed tenure protections and appointment transparency.

3. Problem: The government can exempt itself from key provisions under the pretext of:

a. National security

b. Sovereignty & public order

c. Prevention of crime

i. Why it Matters:
There are no safeguards to prevent mass surveillance or misuse of personal data by state agencies.
Unlike GDPR, which imposes strict necessity and proportionality tests, the DPDP Act gives the government unrestricted exemptions.

ii. Solution: Introduce judicial oversight and require transparency reports on government data requests.

4. Problem: Individuals cannot challenge AI-driven decisions or opt out of automated profiling.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

a. Why it Matters: AI models profile individuals for creditworthiness, insurance, and employment without explanation or human review. GDPR provides a right to contest AI-driven decisions (Article 22), but DPDP does not.

b. Solution: Add a Right to Explanation & Opt-Out from Automated Profiling to ensure AI accountability.

5. Problem: The Act does not differentiate between regular data collection and AI training data.

a. Why it Matters: AI models train on personal data, but the Act does not require explicit consent for AI training. GDPR mandates clear, purpose-specific consent, while DPDP's consent model is vague.

b. Solution: Require separate, opt-in consent for AI training using personal data.

6. Problem: The DPDP Act does not mandate local storage of personal data.

a. Why it Matters: India previously proposed strict data localization laws (2018 & 2019 drafts) but removed them from the final Act. Foreign AI companies (e.g., OpenAI, Google) can store & process Indian data abroad, reducing regulatory oversight.

b. Solution: Introduce sector-specific data localization rules for critical industries (finance, healthcare, biometrics).

7. Problem: The Act does not mandate fairness testing for AI models that process personal data.

a. Why it Matters: AI models inherit biases from training data, disproportionately harming marginalized communities.
GDPR & US AI regulations require fairness testing, but DPDP ignores AI bias issues.

b. Solution: Require AI models to undergo fairness and bias audits before deployment in sensitive areas (e.g., hiring, lending).

8. Problem: The Act only covers digital personal data and excludes non-digital records (Section 3).

a. Why it Matters: Personal data in physical form (e.g., medical records, police files) is not protected. GDPR protects all personal data, regardless of format. Solution: Expand coverage to include non-digital personal data.

9. Problem: The Act does not allow users to transfer their data between services.

a. Why it Matters: Users are locked into platforms (e.g., financial services, cloud storage) with no ability to migrate data.
GDPR grants the right to data portability (Article 20), but DPDP does not.

b. Solution: Introduce data portability rights, allowing users to export their personal data.

10. Problem: Users cannot demand the removal of their personal data from public sources.

a. Why it Matters: AI models scrape public data (e.g., from social media, government websites).
GDPR provides the Right to Be Forgotten (Article 17), allowing individuals to request deletion.

b. Solution: Allow individuals to remove personal data from publicly available sources.

In Short, The DPDP Act does not regulate the following aspects of AI innovation, meaning there is no restriction under this law on:

- AI training on non-personal data – The Act only applies to personal data. AI models trained on anonymized or synthetic data are not regulated.
- AI-generated content – The Act does not cover AI-generated text, images, or videos unless they contain personal data.
- AI bias, discrimination, or fairness – The law mandates accuracy in personal data

processing but does not regulate algorithmic fairness.

- Publicly available data – If a Data Principal makes their data public, AI systems can process it without restrictions (Section 3(c)).
- Government AI projects – The Act allows government exemptions for sovereignty, public safety, or research (Section 17(2)).

Insights gained

After studying the Digital Personal Data Protection (DPDP) Act, 2023, and its implications for AI innovations, the following key insights emerge:

1. **AI-specific regulations must be layered on top of DPDP to address bias, transparency, and accountability** because the DPDP Act provides a foundational data protection framework but it does not explicitly regulate AI, automated decision-making, or algorithmic fairness, leaving loopholes for AI-driven profiling, bias, and opaque decision-making.

2. The Data Protection Board of India is established for enforcement but is not independent as its members are appointed by the Central Government, creating a risk of selective enforcement and political influence. Government agencies can exempt themselves from compliance under Section 17, raising concerns about mass surveillance and unchecked state access to data. So, **Without an independent regulator, data privacy could become a selective privilege rather than a guaranteed right.**

3. **AI developers have free rein over public data in India, which could lead to ethical concerns in facial recognition, surveillance, and behavioral profiling**. The DPDP Act allows AI models to process publicly available data without restrictions (Section 3(c)). Unlike GDPR, which protects public personal data, DPDP lets AI systems scrape, store, and use publicly available information without consent.

4. Without transparency in AI decision-making, individuals in India could face discrimination, financial exclusion, or bias with no legal recourse as the Act does not grant individuals the right to contest AI-driven decisions (e.g., credit scoring, hiring, insurance risk assessment) unlike GDPR which mandates a 'Right to Explanation' for AI-based decisions, ensuring accountability.

5. **Once personal data enters AI training datasets, individuals lose control over how it is used, stored, or repurposed**. Unlike GDPR, the DPDP Act does not allow individuals to demand deletion of their personal data from public sources.

6. **AI-driven decision-making in India could reinforce discrimination without oversight, leading to biased credit approvals, job rejections, or wrongful profiling** because The DPDP Act does not mandate fairness audits for AI models used in finance, hiring, healthcare, or surveillance. GDPR & US AI regulations require bias testing and fairness assessments for high-risk AI applications.

7. India requires strict data localization, prioritizing economic growth over national data sovereignty.(The recent DPDP Rules, 2025 draft introduces data localization)

8. A balanced approach is needed—protecting minors while allowing ethical AI research in education.

9. The DPDP Act favors business growth over individual rights, which could lead to unchecked AI expansion at the cost of consumer privacy.

10. India is moving towards global data privacy standards but lags in AI ethics, transparency, and user control.

Conclusion

The Digital Personal Data Protection (DPDP) Act, 2023 marks a significant step forward in India's journey toward a structured data privacy regime. By enforcing lawful processing, consent requirements, and security safeguards, it lays a

strong foundation for protecting personal data in an increasingly digital world. As AI continues to evolve, seamlessly integrating into finance, healthcare, hiring, and governance, the need for robust AI-specific regulations becomes more urgent.

While the DPDP Act effectively regulates personal data processing, it fails to address key challenges posed by AI innovations. It does not regulate automated decision-making, lacks transparency mandates for AI models, and fails to give individuals rights over AI-driven profiling. The absence of data portability and a Right to Explanation leaves users with little control over how AI systems process their personal information.

At the same time, the Act is business-friendly, allowing cross-border data flows and minimizing compliance burdens on startups. However, this approach also introduces risks, such as the lack of independent regulatory oversight and the government's ability to exempt itself from compliance, raising concerns about mass surveillance and selective enforcement.

For India to emerge as a global AI leader, the DPDP Act must evolve to introduce AI governance mechanisms that ensure fairness, accountability, and user rights. Key improvements could include:

- A Right to Explanation for AI-driven decisions.
- Opt-out options for AI profiling and targeted data usage.
- Mandatory fairness audits for AI models handling sensitive personal data.
- Judicial oversight on government data access.
- Regulating AI's use of public data to prevent unethical data scraping.

Without these reforms, India risks falling behind in AI governance, allowing unchecked algorithmic bias, opaque decision-making, and mass data exploitation. The DPDP Act provides a solid starting point, but to truly balance innovation with privacy, it must evolve into a comprehensive framework that regulates not just data, but how AI systems use it.

The future of AI in India depends not just on innovation, but on responsible regulation that protects individuals while fostering technological growth. The DPDP Act is a step in the right direction—but it must not be the final step.