IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Artificial Intelligence And Data Privacy: Are India's Laws Strong Enough For The AI Era?

**Ishani Thakur, 2Dr. Nitu Singh**
**Student**
**Chandigarh University**

**Keywords:** AI, data protection, personal information, consent, algorithmic fairness, profiling, surveillance, biometrics, Aadhaar, DPDPA 2023, IT Act 2000, privacy rights, ethical AI.

## Introduction

AI is now everywhere from chatbots that write emails to cameras that recognise faces in crowds, from credit-score algorithms to police prediction tools. Each of these systems runs on massive amounts of personal data. In India, where a billion-plus people are rapidly going digital, this creates both opportunity and danger. Data leaks, biased decisions, hidden profiling, and state surveillance can erode dignity and equality. The central question is simple: do our laws keep pace with these risks? This piece maps the legal landscape, highlights real-world problems, spots the gaps, and suggests practical fixes.

## Part I – What Laws Do We Actually Have?

India still lacks a single, GDPR-style privacy law that covers every kind of data use. Instead, protection comes in patches.

1. **Information Technology Act, 2000 (IT Act)**

- Section 43A makes companies liable if they mishandle "sensitive personal data" (passwords, bank details, health records, biometrics, etc.) and cause harm through negligence.
- The 2011 SPDI Rules spell out what counts as sensitive and demand "reasonable" security.
- Sections like 66E punish unauthorised capture of private images, but these are criminal provisions, not everyday remedies. **Catch:** Only companies are covered, not government bodies. Non-sensitive data (your shopping habits, location pings) falls outside. Enforcement has been weak.

2. **Digital Personal Data Protection Act, 2023 (DPDPA)**

- Passed in August 2023, finally notified in 2024–25.
- It Covers **digital** personal data (anything that can identify you, stored electronically).
- Introduces two key players:
  - **Data Principal** = you, the individual.
  - **Data Fiduciary** = any entity (company, app, government department) that decides why and how your data is used.

- Core rules: clear notice + freely given consent; purpose limitation; data minimisation; right to correct or erase; right to nominate someone to claim your data after death.
- Children's data gets extra protection—no tracking or targeted ads, parental consent mandatory.
- Cross-border transfers allowed except to blacklisted countries.
- A new Data Protection Board will investigate complaints and impose fines up to ₹250 crore. **Missing pieces:**No full "right to be forgotten", no data portability, no mandatory explanation when algorithms make life-changing decisions.

3. **AI-Specific Guidance (non-binding but influential)**

- NITI Aayog's #AIForAll strategy (2018, updated 2022) called for fairness audits and open data for public good.
- IndiaAI portal stresses that AI systems must respect privacy-by-design and allow human oversight in high-stakes cases.

**Part II – When Things Go Wrong in Real Life**

- **2024–25 leaks via generative AI:** Doctors and lawyers typed Aadhaar numbers, PAN cards, and medical reports into ChatGPT/Claude/Gemini. Within weeks, this data appeared for sale on dark-web markets.
- **Karnataka school facial recognition (2024):** 1.2 million children's faces linked to a central database for attendance. No public audit of accuracy across skin tones, no clear optout for parents.
- **Finance Ministry circular (Jan 2025):** Banned officials from using foreign AI tools for any file containing personal data—after sensitive budget drafts were found in US servers.
- **Delhi Police predictive policing pilot:** Flagged "habitual offenders" using old crime data, disproportionately targeting certain colonies. No transparency on how the model was trained.

These are not hypothetical; they are headlines from the last 18 months.

**Part III – The Gap Analysis**

**What works**

- DPDPA finally gives every Indian enforceable rights over their digital footprint.
- Heavy penalties will hurt big tech pockets.

- Children's provisions are world-class on paper.

**What doesn't**

1. **Government exemption risk:** Section 17(2) allows the Centre to exempt "any instrumentality of the State". Surveillance drones, smart-city cameras, and social-registry AI could escape the same rules that bind Swiggy or Paytm.
2. **No handle on algorithmic harm:** If an AI denies you a loan or flags you as "high risk", you have no legal right to see the logic or challenge the training data.
3. **Consent theatre:** Tick-box notices written by lawyers are not genuine choice when the service is essential (banking, Aadhaar-linked welfare).
4. **State capacity:** The Data Protection Board is still being staffed. India has ~1 privacy professional per 2 million citizens—compare to 1 per 50,000 in the EU.
5. **Cross-border reality:** Most powerful AI models live in Virginia or Shanghai. Indian law claims extraterritorial reach, but serving a ₹250 crore fine on a US AI lab is easier said than done.

**Part IV – Recommendations That Can Actually Be Implemented**

1. **Tiered risk framework** ○ Low risk (chatbots) → light registration.
   ○ High risk (recruitment AI, criminal justice AI) → mandatory third-party audit + public summary of bias tests.
2. **Algorithm explainability clause** Amend DPDPA Section 7 to add: "Where automated processing produces legal effects, the data principal shall have the right to a humanreadable explanation."
3. **Bring government under the same umbrella** Delete or narrow Section 17 exemptions; make every public-sector AI system file a privacy impact assessment with the DP Board.
4. **National AI incident registry** Like aviation black-box reports—any time an AI causes documented harm (wrongful denial of benefits, discriminatory outcome), the deployer must report within 72 hours.
5. **Funding fix** Allocate 0.1% of the ₹10,000 crore IndiaAI Mission budget to the DP Board and state-level privacy cells.
6. **Digital literacy push** Add one chapter on "Your Data, Your Rights" to Class 9–10 textbooks; run 60-second primetime ads in 12 languages.

**Conclusion**

India now has a modern data-protection law on the books. That is real progress. But AI does not merely move data—it infers, predicts, and sometimes discriminates at scale. Until the law demands transparency from algorithms, binds the state as tightly as it binds startups, and builds enforcement muscle, citizens will remain vulnerable. The DPDPA is a strong foundation; the next Parliament session must lay the missing floors risk-based AI regulation, genuine government accountability, and rights that work against black-box models. Only then will India's billion digital lives be truly protected.