IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Artificial Intelligence And Data Protection: Legal Challenges And The Need For A Robust Framework In India

FIRST AUTHOR- Anurati Dasgupta

LL.M (MASTER OF LAW), UILS, Chandigarh University

SECOND AUTHOR- Dr. Ruchika Sharma

Assistant Professor, UILS, Chandigarh University

ABSTRACT

Artificial Intelligence (AI) has become a central pillar in modern governance, commerce, and social infrastructure. Its potential to analyse massive datasets has revolutionized decision-making, but it has also amplified risks to personal privacy, autonomy, and data protection. India's Digital Personal Data Protection Act, 2023 (DPDP Act) is a crucial step toward safeguarding individual privacy in the digital era. However, the Act does not yet provide a comprehensive response to AI-specific issues such as algorithmic bias, automated decision-making, and data-driven surveillance. This paper critically examines India's emerging data protection regime in comparison with the European Union's General Data Protection Regulation (GDPR) and the EU Artificial Intelligence Act (AI Act). It identifies existing gaps and proposes a multi-layered, risk-based legal framework suited to India's socio-economic and technological context.

Keywords: Artificial Intelligence, Data Privacy, Data Protection, DPDP Act, India.

INTRODUCTION

Artificial Intelligence has revolutionized data driven governance and innovation. However, the interaction with Artificial intelligence and privacy brings up important legal and ethical issues. Artificial Intelligence technologies and tools such as machine learning models, risk analysing tools, predictive analytics and automated decision-making tools are majorly used by various businesses, companies and social work organizations to manage their day-to-day business activities. These AI systems operate by collecting, processing and analysing large amount of personal data, behavioural data and algorithms and they often do not take permission from the user to access the data[1].

[1] Dirk Helbing, "Societal, Economic, Ethical and Legal Challenges of the Digital Revolution: From Big Data to Deep Learning, Artificial Intelligence, and Manipulative Technologies" (2015) https://arxiv.org/pdf/1504.03751/

The Supreme Court of India confirmed the right to privacy as a basic right in Justice K.S Puttaswamy vs. Union of India (2017)[2]. In response, the Indian Parliament passed the DPDP Act 2023, which aims to govern and highlight the processing of digital personal data in a way that acknowledges both individual's right to protect their personal data and necessity to handle such data for authorised purposes[3].

However, the DPDP Act does not specifically add regulatory requirements that are specific to the risk related to specific AI systems, such as algorithm, fairness standards or automated decision making and instead only concentrates on data processing governance. This gap is a significant part that has to be highlighted because traditional data protection regulations might not adequately address the accountability of AI systems and the risks and other related issues that are interconnected with AI and Data privacy regulation. Therefore, India urgently needs a legal framework that addresses the relationship between AI and the protection of personal data[4].

LEGAL FRAMEWORK IN INDIA

The Digital Personal Data Protection (DPDP) Act, which has received president of India's assent on 11th August 2023 replaces earlier legislative attempts like IT Act or Sensitive Personal Data Rules 2011[5]. It applies to digital personal data whether originally collected or digitised subsequently and has extraterritorial application when processing of such data is connected with offering goods or services to data principals in India.

The DPDP Act was adopted[6]:

- Firstly, to replace outdated laws and address the modern data protection challenges that the IT laws failed to address,
- Secondly, the landmark judgement of Supreme court on privacy in Puttaswamy vs UOI in 2017 is a major factor for the adoption of DPDP Act and
- Rapid growth of technology and digital platforms are some of the factors for the adoption of DPDP.
- Permitting the legitimate processing and use of data of an individual by any organization by imposing certain standards that needs to be followed both by the data controller and the individual.

DPDP Act relies on 7 principals:

consented, lawful, and transparent use; purpose limitation; data minimization; data accuracy; storage limitation; reasonable security safeguards; and accountability. These principles guide how organizations can collect, process, and store individuals' personal data while protecting their privacy.

[2] *Justice K.S. Puttaswamy (Retd.) & Anr v. Union of India & Ors.* (2018) https://desikaanoon.in/wp-content/uploads/2024/11/Justice_K_S_Puttaswamy_Retd_vs_Union_Of_India_on_26_September_2018.pdf

[3] Government of India, *"Digital Personal Data Protection Act, 2023"*, available at: https://dpdpact2023.com/index (last visited 1 November 2025).

[4] *"AI and Data Privacy: Creating a Robust Legal Framework in India"* (WithLaw, 2025) https://withlaw.co/blog/Technology-and-Innovation-1/AI-and-Data-Privacy:-Creating-a-Robust-Legal-Framework-in India#:~:text=Comparatively%2C%20India's%20approach%20can%20be,its%20unique%20socio-economic%20context.&text=While%20India's%20Digital%20Personal%20Data,protection%20laws%20alone%20cannot%20resolve. accessed 7 November 2025

[5] Nishith Desai Associates, *India's Digital Personal Data Protection Act, 2023: History in the Making*, Hotline – Technology Law Analysis, 7 Aug. 2023, https://nishithdesai.com/research-and-articles/hotline/technology-law-analysis/indias-digital-personal-data-protection-act-2023-history-in-the-making 10703#:~:text=India's%20Digital%20Personal%20Data%20Protection,them%20in%20the%20DPDA%20itself

[6] Chambers and Partners, *"S & R Data+ India's New Law: The Digital Personal Data Protection Act, 2023"*, 1 Sept 2023, available at: https://chambers.com/articles/s-r-data-india-s-new-law-the-digital-personal-data-protection-act-2023 (last visited 4 Nov 2025).

The statute adopts the following 7 principle[7]-

1. **Consent, lawfulness and transparency**- Data Principal or any individual whose personal data is being processed must give free, informed and specific consent for such processing.
2. **Purpose Limitation-** The personal data must be used strictly for the purpose for which it has been collected.
3. **Data Minimization-** Only minimum necessary data should be collected for the specific purpose thereby reducing the risk of data misuse.
4. **Accuracy-** It must be ensured that the data is accurate and kept up to date.
5. **Storage Limitation-** The data should not be stored after it has been used for the specific purpose.
6. **Reasonable Security Safeguards-** Organizations must implement appropriate technical and organizational measures to ensure confidentiality and integrity of the data and also to protect the data from unauthorized access.
7. **Accountability –** Organizations or companies processing personal data must be held liable for non-compliance and penalties in case of data breach.

Certain important areas that the DPDP covers are: The DPDP provides rights for data principal and obligations for data fiduciary. The Key provisions include:

- **Definitions:** Although many concepts in the DPDP Act closely resemble those found in the EU's General Data Protection Regulation (GDPR), framework, there are differences in how terminology is used. The DPDP defines the following[8]:

  a) Data fiduciary: This refers to the entity that, either independently or in collaboration with others, establishes both the purpose and the methods for processing personal data (similar to a data controller). The government can classify any data fiduciary or a specific group of data fiduciaries as 'significant data fiduciaries' (SDFs). The criteria for this classification as an SDF includes he nature of processing activities (such as the volume and sensitivity of personal data involved and the potential impact on data principals' rights) to broader societal and national concerns (such as the potential effects on India's sovereignty and integrity, electoral democracy, state security, and public order). The designation of SDF comes with heightened compliance obligations as explained below.

  b) Data processor: This is an entity responsible for processing digital personal data on behalf of a data fiduciary.

  c)Data principal: These are individuals whose personal data is gathered and processed (equivalent to a data subject).

  d) Consent manager: A person registered with the Data Protection Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw their consent through an accessible, transparent, and interoperable platform.

- **Applicability**: The DPDP Act applies to all data, whether originally online or offline and later digitized, in India. Additionally, the Act applies to the processing of digital personal data beyond India's borders, particularly when it encompasses the provision of goods or services to individuals within the Indian territory[9].

[7] Taxmann Publications, *"Overview of Digital Personal Data Protection Act (DPDP Act) 2023"*, Blog | Company Law, 4 May 2025, https://www.taxmann.com/post/blog/overview-of-digital-personal-data-protection-act-dpdp-act

[8] Cayman Rayner & Shinjini Kaushal, *"India's Digital Personal Data Protection Act, 2023: Key Provisions"*, India Briefing (18 Sept 2023), available at: https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html?utm_source=chatgpt.com (last visited 1 Nov 2025).

[9] Anand, Khyati & Cyrill, Melissa, *"India's Digital Personal Data Protection Act, 2023: Key Provisions"*, India Briefing (18 Sept 2023), available at: https://www.india-briefing.com/news/indias-digital-personal-data-protection-act-2023-key-provisions-29021.html (last visited 4 Nov 2025).

The provisions of the DPDPA do not apply to (i) personal data processed by an individual for personal or domestic purposes, and (ii) personal data that is made or caused to be made publicly available by (a) the data principal to whom such personal data relates, or (b) any other person who is under a legal obligation to make personal data publicly available[10].

- **Processing of personal data (Section 4):** The personal data of a data principal can only be processed by a person when the data principal has given her consent to use such data for a legitimate or lawful purpose[11].
- **Notice and Consent (Sections 5 and 6):** The consent given by the data principal must be free, specific, informed, unconditional, unambiguous and written in clear language. When processing is based on consent, the data principal has the right to withdraw that consent at any time and the data fiduciary shall, within a reasonable time, cease such processing of personal data. Now, along with the consent, the data fiduciary must provide a notice to the Data Principal containing specified details and it must also explain how the data principal can register a complaint with the Data Protection Board of India[12].
- **Certain Legitimate Uses (Section 7):** Processing without consent is permitted only in certain conditions[13]:

  -Data Principal has voluntarily provided her personal to Data Fiduciary for specified purpose.

  -For state function in relation to providing government benefit, certificate, license, subsidy to the Data Principal.

  -to fulfil any legal obligation

  for compliance to any judgement or decree or order by the court

  -for responding to a medical emergency that involves threat to life

  -for measures to ensure safety of any individual during disaster

- **Data Fiduciaries have Certain Obligations that includes[14]: (Section 8)**
  -ensuring the completeness, accuracy and consistency of personal data

  -undertaking reasonable security safeguards to prevent a data breach;

  -informing the Board and the affected data principal in the event of a breach; and

  -erasing personal data as soon as the specified purpose has been met and retention is not necessary for legal purposes.

---

[10] Nishith Desai Associates, *India's Digital Personal Data Protection Act, 2023: History in the Making*, Hotline – Technology Law Analysis, 7 Aug. 2023, https://nishithdesai.com/research-and-articles/hotline/technology-law-analysis/indias-digital-personal-data-protection-act-2023-history-in-the-making 10703#:~:text=India's%20Digital%20Personal%20Data%20Protection,them%20in%20the%20DPDA%20itself

[11] Ministry of Electronics & Information Technology (MeitY), *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*, Gazette of India (11 August 2023), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[12] Ibid

[13] Ministry of Electronics & Information Technology (MeitY), *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*, Gazette of India), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[14] Chambers and Partners, *"S & R Data+ India's New Law: The Digital Personal Data Protection Act, 2023"*, 1 Sept 2023, available at: https://chambers.com/articles/s-r-data-india-s-new-law-the-digital-personal-data-protection-act-2023 (last visited 4 Nov 2025).

- **Processing of personal Data of Children (Section 9):** Before processing any personal data of a child, the Data Fiduciary must obtain consent from the parent of the child. The Data Fiduciary should not process such data, which can be detrimental to the child's wellbeing and also should not track or monitor the children's behaviour or any other activity[15].
- **Data Principles have certain rights and duties (Section 11-14):**

  -Data has right to access information about personal data,

  -Has the right to erasure and correction of personal data on request of the Data Principal

  -Has right to grievance redressal- the Data Principal has the right to complain to Data Fiduciary if rights have been violated and further this can be taken to the Data Protection Board of India[16].

  -Data Principal has the right to nominate one or more individuals to exercise her right on behalf of the Data Principal in case of incapacity or death.

  -Data Principal can withdraw consent given to the Data Fiduciary to process data.

  -The data Principal can manage, review, and withdraw consent anytime through the consent manager, who acts on behalf of the Data Principal.

NITI AAYOG'S NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE:

The government-run think tank National Institution for Transforming India, or "NITI Aayog," has been entrusted with creating a national AI strategy to guide the government's AI initiatives[17]. Early in May 2018, NITI Aayog and Google partnered to teach and support start-ups looking to create and incorporate AI-based solutions into their business models in an attempt to increase economic productivity in India [18]. In late May 2018, NITI Aayog and ABB India signed a declaration of intent to "realize the potential of AI, big data, and connectivity and make key sectors of the Indian economy ready for a digitalized future. NITI Aayog outlines the main objective for a nationwide discussion paper published in June 2018[19].

The main objective of a national AI strategy, according to NITI Aayog's June 2018 discussion paper [20], is to "leverage AI for economic growth, social development and inclusive growth, and finally as a "Garage" for emerging and developing economies." NITI Aayog's engagement goes beyond only suggesting a policy approach; it also involves deployment and implementation. In two key aspects, the National Strategy surpasses all previous AI policy processes. First, it recognizes the "need to strike a balance between narrow definitions of financial impact and the greater good" and the fact that the adoption of AI has so far been

[15] Ministry of Electronics & Information Technology (MeitY), *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*, Gazette of India https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[16] Ministry of Electronics & Information Technology (MeitY), *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*, Gazette of India https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[17] Sharma, Yogima Seth & Agarwal, Surabhi, *"Niti Aayog to come out with national policy on artificial intelligence soon"*, *The Economic Times*, 21 Mar. 2018, available at: https://economictimes.indiatimes.com/news/economy/policy/niti-aayog-to-come-out-with-national-policy-on-artificial-intelligence-soon/articleshow/63387764.cms (last visited 8 Nov. 2025).

[18] Gupta, Komal, *"NITI Aayog Partners with Google to Grow India's Artificial Intelligence Ecosystem"*, *Mint* (7 May 2018), available at: https://www.livemint.com/Industry/fpnGnNQ8duTCRZOEpk2P6M/Niti-Aayog-partners-with-Google-to-grow-Indias-artificial-i.html (last visited 8 Nov 2025).

[19] NITI Aayog, *National Strategy for Artificial Intelligence: #AI for All* (Discussion Paper, June 2018), NITI Aayog, p. 46, available at: http://www.niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf (last visited 8 Nov 2025).

[20] NITI Aayog, *National Strategy for Artificial Intelligence: #AI ForAll* (June 2018), available at: https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf (last visited 8 Nov 2025).

mostly driven by commercial interests. Second, it acknowledges that AI applications should be welcomed for their incremental benefits rather than their alleged transformative potential across a range of industries.

The substantive proposals and analysis of India's national strategy on AI fall short, notwithstanding these positive changes in viewpoint. The study cites five main areas education, agriculture, healthcare, smart cities and infrastructure, and smart mobility and transportation where AI might have a beneficial societal impact and where the government must take the lead.

These include social media intelligence platforms that can support public safety, "sophisticated surveillance systems" that could monitor people's movement and behaviour, and AI systems that can forecast crowd behaviour and be utilized for crowd management. The report's suggestions regarding smart cities did not address the serious constraints of accuracy and fairness as well as the detrimental effects of surveillance on fundamental rights. This is especially concerning because India's monitoring system already lacks sufficient protections to prevent law enforcement officials from potentially eroding fundamental liberties[21]. Therefore, AI-powered monitoring need to be the exception rather than the rule. It is essential to comprehend and modify these systems for the social context in which they will operate in order to lessen bias within them. In fact, preventing discriminatory results should be the goal. Eubanks has noted that the employment of automated decision-making technologies will only exacerbate systemic injustices unless they are designed to eliminate them[22].

JUDICIAL PRECEDENTS SHAPING DATA PROTECTION IN INDIA

1. Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017):

The Right to Privacy was made a basic right under Article 21 of the Indian Constitution by this landmark Supreme Court ruling. The Aadhaar plan, which compelled people to provide biometric and demographic information in order to access government services, was challenged, thereby which led to the case[23].

Judgment: The Court held that privacy is intrinsic to life and liberty, emphasizing that data collection and processing must adhere to principles of necessity and proportionality. The ruling underscores the importance of safeguarding personal data against misuse by both private entities and the State, forming the bedrock for interpreting the DPDP Act in AI-related cases[24].

2. Shreya Singhal vs. Union of India (2015):

While primarily addressing freedom of speech under Section 66A of the IT Act, this case highlighted the risks of vague legislative provisions in regulating digital technologies.

---

[21] Bailey, R., Bhandari, V., Parsheera, S. & Rahman, F., *Use of Personal Data by Intelligence and Law Enforcement Agencies*, Macro/Finance Group, National Institute of Public Finance and Policy (Aug. 2018), available at: https://macrofinance.nipfp.org.in/PDF/BBPR2018-Use-of-personal-data.pdf (last visited 8 Nov. 2025).

[22] Eubanks, Virginia, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (2018), New York, NY: St. Martin's Press, available at https://us.macmillan.com/books/9781250074317/automatinginequality/

[23] Kashyap, Trisha, *"The Intersection of AI and Data Privacy: Challenges Under India's Digital Personal Data Protection Act, 2023"*, Lawful Legal (18 March 2025), available at: https://lawfullegal.in/the-intersection-of-ai-and-data-privacy-challenges-under-indias-digital-personal-data-protection-act-2023/ (last visited 4 Nov 2025).

[24] Justice K.S. Puttaswamy (Retd.) vs. Union of India, (26 Sept. 2018) (India), available at: https://desikaanoon.in/wpcontent/uploads/2024/11/Justice_K_S_Puttaswamy_Retd_vs_Union_Of_India_on_26_September_2018.pdf (last visited 27 Sept 2025).

Judgment: Section 66A was overturned by the Supreme Court due to its excessive broadness and ambiguity. The decision serves as a warning about the DPDP Act's ambiguous and undefined terms, such "public interest," which could be abused to support invasive AI applications[25].

3. Anvar P.V. vs. P.K. Basheer (2014):

This case dealt with the admissibility of electronic evidence in courts, emphasizing the need for authenticity and consent in collecting such data.

Judgment: The Court emphasized how important it is to make sure that electronic data especially data processed by artificial intelligence, complies with stringent evidentiary requirements. This ruling emphasizes how AI-driven data breaches may affect court cases[26].

4. Lalita Kumari vs. Govt. of Uttar Pradesh (2013):

Facts: This case dealt with the mandatory registration of FIRs by police authorities and the use of technology in surveillance and policing.

Judgment: The ruling warned against intrusive surveillance methods that can infringe on people's privacy, even if it affirmed the necessity of efficient law enforcement. This speaks to worries about the use of AI-powered facial recognition software without sufficient security[27].

GAPS IN THE INDIAN LEGAL FRAMEWROK IN RELATION TO AI AND DATA PRIVACY

At the intersection of AI and personal data protection India's DPDP Act fails to address specific regulations for AI-driven issues and challenges like algorithm bias and transparency. Other challenges include loopholes in addressing mass surveillance, difficulties in obtaining truly informed consent for complex AI systems, and the potential for data breaches and misuse, particularly in the context of cross border data transfers. Additionally, the existing framework fasces issues with accountability gaps for AI powered decisions.

The recent AI startups in India face the challenge of accessing language, health, and consumer data while following legal obligations set by the government. Since the DPDP lacks explicit rules regulating anonymised data, this creates a grey governance area. However, there are no international standards regulating the deanonymisation effort[28].

The major gaps are:

a) **Lack of AI-Specific Regulations:** Although general recommendations for protecting personal data are provided under India's data privacy regulations that is DPPD Act 2023 but the specific important

[25] Shreya Singhal v. Union of India, Writ Petition (Criminal) No. 167 of 2012, decided 24 Mar. 2015 (Supreme Court of India), available at: https://indiankanoon.org/doc/110813550/ (last visited 8 Nov. 2025).
[26] Anvar P.V. v. P.K. Basheer & Ors, (18 Sept 2014) (India), available at: https://indiankanoon.org/doc/187283766/ (last visited 8 Nov. 2025).

[27] Choudhary, Harish, *"Lalita Kumari v. Govt. of U.P.: Touching Upon Untouched Issues"*, (2014) Nirma University Law Journal Vol. 3 Issue 1, pp. 99–108, available at: https://docs.manupatra.in/newsline/articles/Upload/FD30EC39-2367-4E2E-B088-01FA06971A5E.%20GOVT%20OF%20UTTAR%20PRADESH%20%20TOUCHING%20UPON%20UNTOUCHED%20ISSUES.pdf (last visited 8 Nov 2025).

[28] Observer Research Foundation (ORF), *"India at the Crossroads: Balancing Data Localisation, Privacy and AI Innovation"*, available at: https://www.orfonline.org/expert-speak/india-at-crossroads-balancing-data-localisation-privacy-and-ai (last visited 9th Nov 2025).

requirements of AI systems are not taken into consideration. In order to improve their algorithms and performance, AI models need constant access to large datasets which can result in data breach and misuse of an individual's personal information as the data can be utilized for purpose that the individual did not provide their express consent. As AI systems constantly develop themselves therefore it becomes difficult to guarantee that the data used to train these models is protected[29].

b) **Cross Border data transfers**: The transmission of personal data of an individual from one nation to another for processing or storing for a specific purpose is known as cross-border data transfer. For companies that employ cloud-based services, outsource data processing or conduct business internationally, these kinds of transfers are important. The DPDP sets out specific conditions and restrictions for governing cross-border data flow as seen under Section 16(1) which allows Central government to regulate data transfer by backlisting such countries whose data protection regime is weak or inadequate or where national security concern arises. But this section lacks clarity as businesses find it challenging to anticipate regulatory constraints due to the lack of transparency surrounding the criteria for whitelisting and blacklisting countries[30]. Therefore, it can be said that DPDP Act attempts to address cross-border data transfer but fails to fully address account for the risks posed by the transnational nature of AI systems, which may operate across borders in ways that undermine India's data protection laws[31]. Therefore, balancing data protection with cross border data flow for business transactions remains a key challenge mainly for the organizations operating across different jurisdictions[32].

c) **Accountability and Transparency:** The DPDP Act does not provide mandate for AI explainability that is the ability to understand how an AI has reached certain decision. Thus, AI being opaque, it becomes a threat to users. Many AI models are "black boxes" which confuses and makes difficult for users to understand and identify the decision-making process used by AI which leads to concerns about transparency, fairness and potential bias in areas like hiring, law enforcement, healthcare, business etc[33]. For example, opaque algorithms could determine credit scores or employment decisions without clear justification, undermining accountability. The existing legal framework that is the DPDP Act fails to address the accountability that is who is to be held accountable for such AI driven decisions and transparency in regards to such decision making. Therefore, absence of accountability for the developers and deployers of AI systems further leads to need for a strong legal framework[34].It does not impose any direct obligations on developers or deployers of AI to disclose

[29] Naik, Anjali Gurunath, *"Data Privacy in India's AI Boom: Are We Protecting What Matters?"*, LJRF Voice (blog), 1 month ago, available at: https://ljrfvoice.com/data-privacy-in-indias-ai-boom-are-we-protecting-what-matters/#042bd728-a1dc-421a-ac5a-4f85a1115fe0 (last visited 4 Nov 2025).

[30] Data Secure, *"Impact of the Digital Personal Data Protection (DPDP) Act on Cross-Border Data Transfers"*, DPO India Blog, 27 June 2025, available at: https://www.dpo-india.com/Blogs/impact-dpdpa-crossborder/#:~:text=The%20Digital%20Personal%20Data%20Protection%20(DPDP)%20Act%20raises%20several%20concerns,rules%20and%20navigate%20jurisdictional%20overlaps. (last visited 1 November 2025).

[31] Anjali Gurunath Naik, *"Data Privacy in India's AI Boom: Are We Protecting What Matters?"*, LJRF Voice (2025), available at: https://ljrfvoice.com/data-privacy-in-indias-ai-boom-are-we-protecting-what-matters/#042bd728-a1dc-421a-ac5a-4f85a1115fe0 (last visited 4 Nov 2025).

[32] Data Secure, *"Impact of the Digital Personal Data Protection (DPDP) Act on Cross-Border Data Transfers"*, DPO India Blog, 27 June 2025, available at: https://www.dpo-india.com/Blogs/impact-dpdpa-crossborder/#:~:text=The%20Digital%20Personal%20Data%20Protection%20(DPDP)%20Act%20raises%20several%20concerns,rules%20and%20navigate%20jurisdictional%20overlaps. (last visited 1 November 2025).

[33] Naik, Anjali Gurunath, *"Data Privacy in India's AI Boom: Are We Protecting What Matters?"*, LJRF Voice (blog), published 2 months ago, available at: https://ljrfvoice.com/data-privacy-in-indias-ai-boom-are-we-protecting-what-matters/#042bd728-a1dc-421a-ac5a-4f85a1115fe0 (last visited 4 November 2025).

[34] Ibid

how algorithmic decisions are made. Examples like biometric failures in welfare schemes highlight how automated systems can cause harm without a clear redressal mechanism for algorithmic discrimination.

d) **Broad Exemptions for Government Processing:** The DPDP Act provides provision that allows processing of data by government instrumentalities for sovereignty, security and public order without consent from the data principal. This raises concerns of surveillance risk and oversight in public sector AI deployments[35]. Th exemptions must be provided in such way so that the data principal does not get harmed.

e) **Automated decision making:** AI's automated decision-making in recruitment, loan approval, financial services, law enforcement or predictive policing can affect the fundamental right of the data principal or user[36]. India's DPDP Act lacks explicit restrictions on solely automated decisions that significantly impact individuals, unlike Article 22 of the GDPR. This results in lack of transparency, biasness and misuse of data. Thus, DPDP lacks to address this gap which is a very essential concern that needs to be addressed.

PRIVACY CONCERNS AND DEMANDS OF USERS IN RELATION AI AND DATA PROTECTION

Individuals can get benefited from personalized AI services that can solve a variety of user-related problems. Simultaneously, these AI services demand the associated personal data of these individuals for example location, password, microphone access etc, thus can discover new information about them which can be sensitive. So, as there is a need for such data intensive AI-services there arises the privacy concerns and it has to be seen as to how privacy can be maintained[37].

PRIVACY CONCERNS:

To further identify and categorize user issues, we first offer a taxonomy of privacy concerns[38]:

- First is the **improper acquisition** which refers to the collection of personal data without users' knowledge or consent, such as through unauthorized access and data collection outside of the service, or covert monitoring of users' online and offline behaviour.
- Secondly, **Inappropriate use and transfer of data**, which relates to the transfer and analysis of personal information without consent. In the former scenario, the analysis of personal data is done to draw conclusion about user behaviour without taking consent from the user. In the latter instance, users' personal information is transferred to third parties without their knowledge or consent. Therefore, one of the main concerns is data transfer. Users are mostly concerned about transfer of their personal data to third parties that often leads to loss of ownership of data as it is collected and used without the user consent.
- **Privacy invasions or violation concerns** relates to sending information to potential users and unwanted execution of tasks without users' acknowledgment or consent are the main types of privacy violations.
- **Improper storage concern -**the AI systems, by their design, accumulate vast datasets for training and optimization, often stored indefinitely across multiple servers and jurisdictions. The absence of

[35] *"India Introduces Digital Personal Data Protection Act 2023"*, Asia IP Law, available at: https://asiaiplaw.com/sector/it-telecoms/india-introduces-digital-personal-data-protection-act-2023? (last visited 26 Sept 2025).

[36] *"Why We Need Data Protection Laws for AI in India"*, De Facto Law Journal (n.d.), available at https://defactolawjournal.org/papers/why-we-need-data-protection-laws-for-ai-in-india/ (last visited 27 Sept 2025). defactolawjournal.org

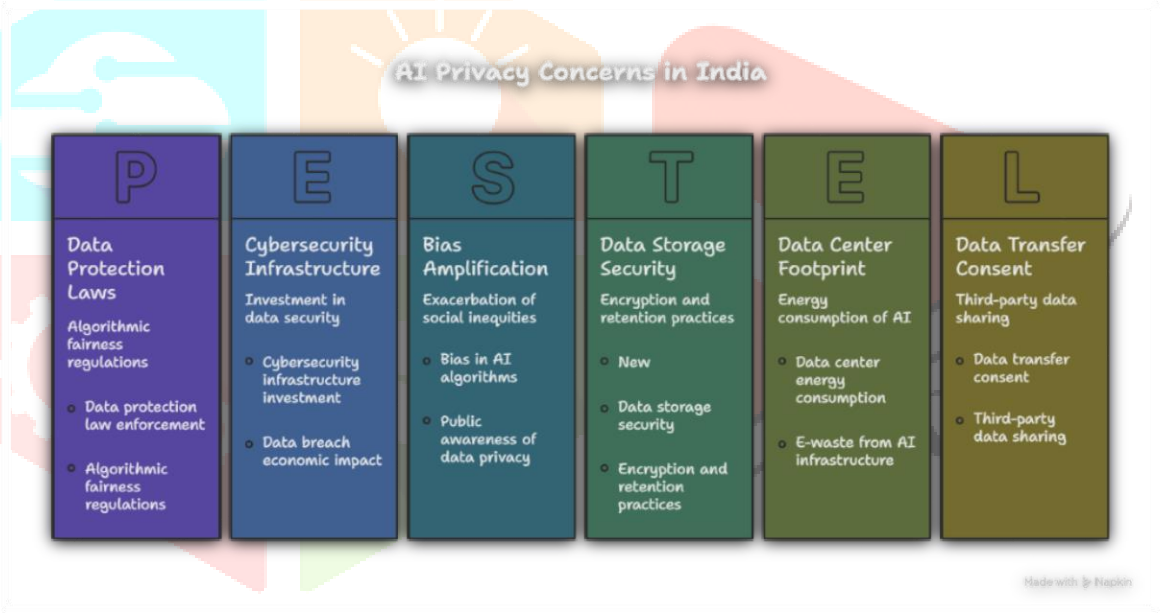
[37] Wang, Huaiqing, Lee, Matthew K. O., and Wang, Chen, *"Consumer Privacy Concerns about Internet Marketing"*, (1998) 41(3) *Communications of the ACM* 63–70, DOI: https://doi.org/10.1145/272287.272299.

[38] Ibid

strict data retention limits or standardized encryption practices increases the vulnerability of personal data to breaches and unauthorized access. In India, where many AI-driven entities lack robust cybersecurity infrastructure, the risk of data leaks or unlawful secondary use is particularly acute. Data integrity and confidentiality issues are linked to improper storage.

- **Bias in AI Algorithms-** AI models can inadvertently perpetuate or amplify bias. As one survey notes, a general AI model is often already "biased towards a certain kind of individual" if the training data reflects existing prejudices. The developers' own assumptions or skewed datasets may lead to unfair outcomes (e.g. underrepresenting minorities in medical data). In India, this could exacerbate social inequities. Where biased AI decisions affect privacy (e.g. filtering of certain demographic data or targeted content), they violate principles of fairness implicit in data protection law. Ensuring algorithmic fairness is thus a legal challenge: without safeguards, AI could discriminate on the basis of race, gender, religion or other sensitive attributes[39].

The privacy of the user is influenced by four factors, namely, the type of data, the type of service, the involvement of third parties and the context of use. For instance, users are less comfortable with the collection of data types such as biometrics (including fingerprints), images, contact information than environmental data (including room temperature and physical presence. The users don't have enough knowledge and understanding of the negative consequences of data collection which leads to the subsequent misuse of data as well[40].



PRIVACY DEMANDS:

The increased use of personal data by AI for various purposes has raised concerns in regards to the protection of such data. Therefore, the users demand data privacy and protection in the following domains[41]:

[39] *"AI and Data Privacy in India: Emerging Legal and Ethical Challenges"*, Cyber Law Consulting (n.d.), available at: https://www.cyberlawconsulting.com/ai_and_data_privacy_in_India.php#:~:text=personal%20data%2C%20creating%20privacy%20risks,raising%20ethical%20and%20legal%20concerns (last visited 27 Sept 2025).

[40] Teltzrow, Maximilian & Kobsa, Alfred, *"Impacts of User Privacy Preferences on Personalized Systems: A Comparative Study"*, in C.-M. Karat, J. Blom & J. Karat (eds.), *Designing Personalized User Experiences for eCommerce* (Kluwer Academic Publishers, Dordrecht, 2004) pp. 315-332, available at https://link.springer.com/chapter/10.1007/1-4020-2148-8_17 (last visited 27 Sept 2025).

[41] Wang, Huaiqing, Lee, Matthew K. O., and Wang, Chen, *"Consumer Privacy Concerns about Internet Marketing"*, (1998) 41(3) *Communications of the ACM* 63–70, DOI: https://doi.org/10.1145/272287.272299.

- **Flexible User Consent-** Users must agree to the terms of services and give free consent to the AI services that they are using in regards to processing of their personal data. Three important aspect that has to be looked into is firstly, the term of service should be clear, concise and contain standardize content that can be understood easily. Secondly, the possible risks and threats should be clearly mentioned in such term of service to make the user aware of such risks specially when personal data is shared. Thirdly, Users should have the flexibility to opt in and out such AI services whenever they feel like.

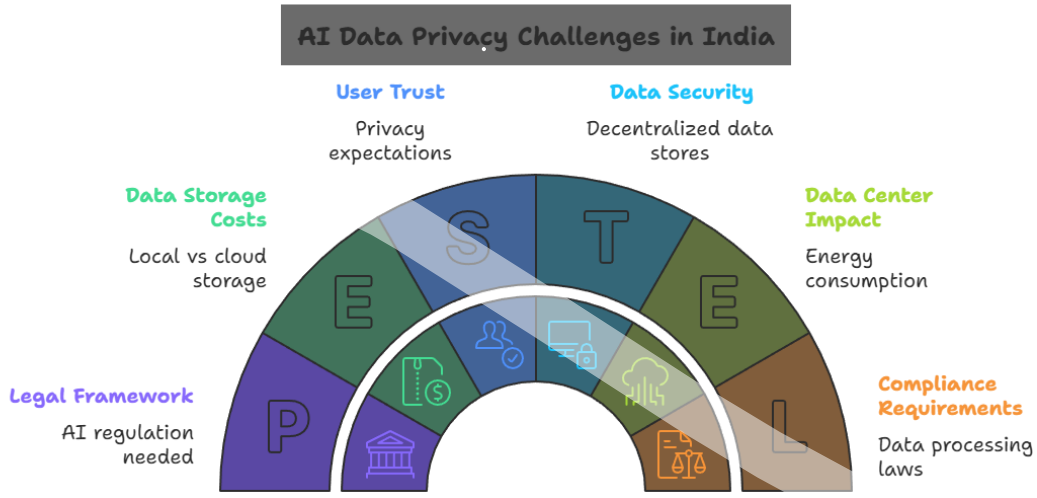
  Conventional privacy law relies on informed consent and limiting data collection. However, AI's thirst for data strains these principles. AI systems often require large datasets sometimes combining disparate data sources to train effective models. Users may not be able to meaningfully consent to all future uses of their data once it is part of a learning model. In practice, organizations must still operate within legal parameters obtaining consent, explaining processing purposes, and ensuring data accuracy[42].

- **Integrity of the context-** Users anticipate contextual integrity from AI services which includes the appropriate actors, data flow, context etc. The personal data collected by the AI systems should be used for the purpose for which it has been collected and not for any other purposes. Thereby necessitating purpose limitation which is a major principal to protect from data breach.

- **Confidentiality:** Users choose local and decentralized data stores over cloud storage for sensitive data as they do not trust the internet services in regards to its security. The three ideal qualities for processing, exchanging and preserving data are data availability, confidentiality and integrity. The AI services using the personal data must ensure all the three ideal qualities before processing of any such data for the specified purpose.
- **Anonimity:** The users always prefer to remain anonymous when data is collected, processed and transmitted. They do not want to reveal their identity as it can be dangerous in regards to their data getting leaked or misused.

Users also expect to know how AI systems use their information and demand options to consent, withdraw, or delete data. Therefore, the increasing use of AI services has led to privacy demands as well as stated above. These privacy demands are necessary to be addressed by the Indian legal framework to ensure a fair and transparent interaction between AI and data that is used by it.

[42] Wadhwa, R., *"Examining India's Efforts to Balance AI, Data Privacy"*, *IAPP* (11 Oct. 2023), available at https://iapp.org/news/a/examining-indias-efforts-to-balance-ai-data-privacy (last visited 27 Sept 2025).



RECOMMENDATIONS: A PROPOSED FRAMEWORK FOR INDIA

The existing legal provisions, such as the DPDP Act, focus narrowly on personal data and do not regulate working of AI systems in data collection and model training to deployment and accountability. To ensure that AI development aligns with data protection principles, India must evolve beyond general privacy laws and incorporate AI-specific laws. The proposed framework should include:

Risk-based AI classification:

Experts stress that India currently has no formal AI risk frameworks. A data driven approach is needed to categorize AI by potential harms such as misuse of personal data, loss of control by the user and other safety risks and also prioritize high risk domains such as healthcare for regulations in India[43]. For example- Google and others has urged an risk based and proportionate approach to AI regulation in India focused on user cases. This will ensure that the risks are targeted and proper safeguard is provided to users or individuals against such risk[44].

Algorithm audits and transparency:

Companies or organizations processing personal data of individuals should conduct audits. Regular internal or independent audits could then check for unintended bias, privacy leaks, or anti-competitive effects. Simultaneously promotion of transparency in AI systems should be done by making mandatory disclosures regarding data utilization, model training methods, and the underlying decision-making processes[45].

The Competition Commission of India (CCI) has recommended that firms maintain algorithmic audit trails recording AI decision-making logic, objectives, and data sources. The Competition Commission of India's

[43] Mohanty, Amlan & Sahu, Shatakratu, *"India's Advance on AI Regulation"*, Carnegie Endowment for International Peace (21 Nov. 2024), available at: https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en (last visited 27 Sept 2025).

[44] Drishti IAS, *"Jharkhand HC Stays on Private Sector Job Quota Law"*, 19 Dec 2024, available at: https://www.drishtiias.com/current-affairs-news-analysis-editorials/news-analysis/19-12-2024 (last visited 27 Sept 2025).

[45] Ibid

(CCI) has recommended enterprises to perform self-audits of their AI systems. Key aspects of the CCI's proposal include[46]:

- Transparent Documentation: Companies should document the AI-based decision-making process, including algorithmic objectives, data sources, and access protocols.
- Safeguards against Unethical Outcomes: The design and testing of AI systems should incorporate built-in safeguards to proactively prevent or detect unintended anti-competitive outcomes, such as algorithmic collusion, predatory pricing, and price discrimination. The CCI report suggests that organizations should build in safeguards (e.g. bias tests) and periodically review outputs to "proactively identify and eliminate inadvertent" harms
- Internal Reviews: The framework suggests regular internal algorithmic audits and periodic reviews of outputs and market outcomes to ensure ongoing compliance.
- Accountability: The proposal encourages clear accountability at senior levels for the deployment and oversight of high-risk AI systems.
- Non-binding Framework: The CCI has clarified that this is a non-binding, voluntary framework intended to help businesses assess risks and integrate competition compliance into their AI design from the outset, rather than a legal requirement at this stage.

These recommendations are part of the CCI's broader "Market Study on Artificial Intelligence and Competition" and aim to ensure responsible autonomy and a level playing field in India's evolving digital economy. Such transparency measures including disclosing the general purpose and main parameters of AI systems would reduce the current "information asymmetry" between AI deployers and individuals or regulators. In short, algorithmic accountability (through audits, documentation, and impact assessments) should be mandated, not left entirely to self-regulation[47].

Privacy/Impact assessments and design safeguards:

Aligning with global best practices, India should require Privacy by Design for AI. This means enforcing data protection impact assessments (DPIAs) or AI-safety assessments before deploying systems that use personal data. Organizations should minimize data use via techniques like anonymization, encryption, differential privacy, or federated learning. As one privacy expert notes, AI-driven services often need data beyond what was anticipated, so pre-emptive DPIAs are crucial. Embedding technical protections (e.g. making privacy the default setting) will help reduce privacy risks. These requirements can be integrated into the DPDP regime by updating its rules or issuing AI-specific guidelines[48].

Oversight and accountability mechanisms:

India should empower its regulators to oversee AI in practice. This could involve expanding the Data Protection Board's mandate or creating a specialized AI review committee. At minimum, any entity deploying high-risk AI should be subject to regulatory supervision and periodic compliance checks. Strengthening the grievance redressal process under the DPDP Act can also help – for instance, explicitly allowing data principals to complain about AI-driven decisions. Transparency obligations (akin to EU requirements) should be codified so that individuals can understand when AI is used in decisions affecting

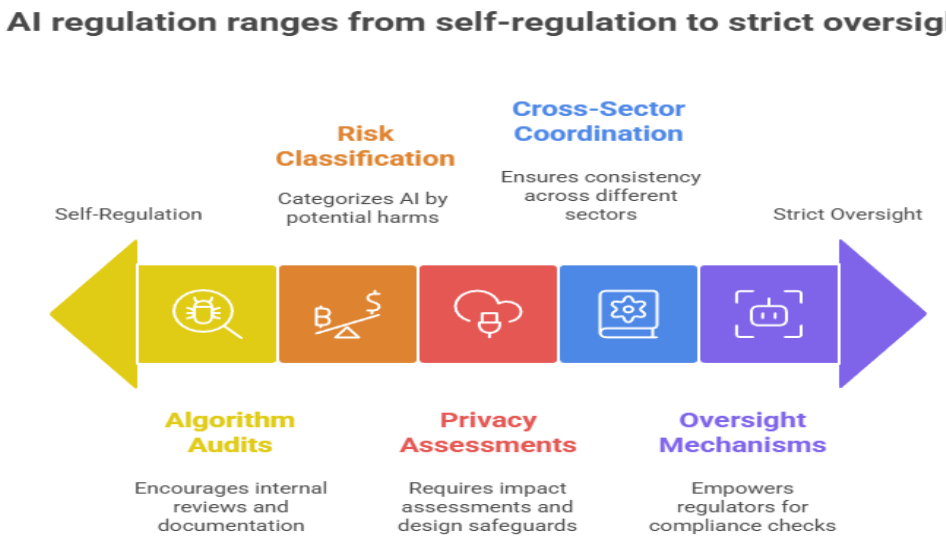
[46] Bansalón, Aakriti, *"Why Competition Commission of India Wants Indian Firms to Self-Audit AI Systems for Competition Risks"*, *MediaNama*, 7 Oct. 2025, available at: https://www.medianama.com/2025/10/223-cci-ai-self-audits-competition-compliance/ (last visited 27 Sept 2025).
[47] Ibid

[48] Wadhwa, R., *"Examining India's Efforts to Balance AI, Data Privacy"*, International Association of Privacy Professionals (11 Oct. 2023), available at: https://iapp.org/news/a/examining-indias-efforts-to-balance-ai-data-privacy (last visited 27 Sept 2025).

them. In short, India needs a clear legal duty for AI developers and users to explain and justify automated decisions. The current lack of algorithmic accountability standards has created a "regulatory void" in India; filling that gap is essential[49].

Cross-sector coordination:

Because AI spans many domains, the framework must be multi-disciplinary. Privacy law should intersect with sectors like credit regulation, health data norms, and anti-discrimination statutes. For example, AI used in hiring could trigger labour or anti-bias laws as well as data rules. Coordinated guidelines (possibly by a multi-ministerial task force) can ensure consistency. Civil society participation and independent audits (as recommended by experts) will also bolster trust[50].



CONCLUSION

AI offers India enormous promise, but its privacy perils are real. Without an integrated AI–data protection framework, individuals risk losing control over their personal information and facing unfair algorithmic outcomes. The DPDP Act 2023 is a welcome foundation for data privacy, but it must be reinforced with AI-specific rules. In particular, India needs to implement transparency and accountability mechanisms (algorithmic audits, impact assessments, clear rights against opaque profiling) and a risk-sensitive regulatory regime for AI. As global experience shows, treating AI as a special case with tailored obligations for high-risk systems is essential to prevent abuses. Ensuring that AI remains "human-centred" will require open disclosure and oversight, not secrecy. In the words of privacy scholars, "to prevent the erosion of data privacy" in the age of AI, mandated disclosures and stakeholder oversight must be pursued[51]. Only by

[49] *"AI and Data Privacy in India: Emerging Legal and Ethical Challenges"*, Cyber Law Consulting (n.d.), available at: https://www.cyberlawconsulting.com/ai_and_data_privacy_in_India.php#:~:text=,to%20ensure%20AI%20ethics%20and (last visited 26 Sept 2025).

[50] Alzghoul, Amro, *"The Impact of Artificial Intelligence on Public Sector Decision-Making: Benefits, Challenges and Policy Implications"*, available at: https://www.researchgate.net/profile/Amro-Alzghoul/publication/394855760_The_Impact_of_Artificial_Intelligence_on_Public_Sector_Decision-_Making_Benefits_Challenges_and_Policy_Implications/links/68f7ecfc02d6215259bda4ff/The-Impact-of-Artificial-Intelligence-on-Public-Sector-Decision-Making-Benefits-Challenges-and-Policy-Implications.pdf (last visited 26 sept 2025)

[51] Mohanty, Amlan & Sahu, Shatakratu, *"India's Advance on AI Regulation"*, Carnegie Endowment for International Peace, 21 Nov. 2024, available at: https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en (last visited 8 Nov. 2025).

embedding robust privacy protections into the AI lifecycle can India safeguard its citizens' rights while harnessing AI's benefits.

While the government is taking various initiatives in respect of AI, the concerns regarding the applicability of existing regulatory frameworks in India, or the adoption of a new law to govern the adoption and use of AI by proactively addressing these concerns, we can ensure that India's legal and regulatory landscape keeps pace with the rapid evolution of this transformative technology[52].

[52] Datta, Ameet, *"Data Privacy Considerations Surrounding AI Use in India"*, *Law.asia* (7 months ago), available at:https://law.asia/ai-and-data protection/#:~:text=The%20DPDP%20Act%20affords%20certain%20rights%20to,right%20to%20correction%2C%20completion%2C%20updating%20and%20erasure (last visited 8 Nov. 2025).