# ARTIFICIAL INTELLIGENCE AND DATA PRIVACY CHALLENGES: A LEGAL PERSPECTIVE

Arokia Sushma, (Research Scholar), Tamil Nadu Dr. Ambedkar Law University

Dr. Ranjit Oommen Abraham, Tamil Nadu Dr. Ambedkar Law University

Dr. R. Haritha Devi, Tamil Nadu Dr. Ambedkar Law University

**ABSTRACT:**

Artificial Intelligence (AI) is revolutionizing economies and societies worldwide by enabling powerful data-driven insights and decision-making. However, there accompanies various data privacy challenges due to AI's demand for large amount of personal data. Concerns like mass surveillance, profiling, bias, and loss of human autonomy arises as information is often gathered, combined, and judged by AI systems. Though new data protection laws have been passed in India, and the right to privacy is ensured under Article 21[1] of the Constitution, conflicts surrounding AI are remarkably high. This article examines AI's effects on data privacy from a legal standpoint, with a focus on India's evolving legislative framework. In the end, we offer strategies (like algorithmic audits, privacy-by-design, and Data Protection Impact Assessments) to strike a balance between the advancement of technology and the right to privacy. India ought to put in place a robust legal system that respects human consent, accountability, and openness. At the same time, the country should avoid unreasonably restricting the advantages of AI as it is highly integrated into industries like healthcare, banking, and governance.

**Keywords:** Artificial Intelligence (AI); Data Privacy; Digital Personal Data Protection Act 2023; Right to Privacy; Algorithmic Bias; Consent; India; GDPR; Facial Recognition; Privacy by Design.

[1] Fundamental Right to Privacy - Supreme Court Observer https://www.scobserver.in/cases/puttaswamy-v-unionof-india-fundamental-right-to-privacy-case-background/

## INTRODUCTION:

Artificial Intelligence (AI) technologies like machine learning, deep learning, and large language models rely on processing large volumes of data, which is often personal[2]. By comprehending data patterns, AI improves automation, predictive analytics, and industry-wide decision-making. AI-driven diagnostic systems, for example, can personalize medical care for each patient, and AIbased finance algorithms can expedite credit lending. A huge socio-economic profit is expected from such capabilities (for example, McKinsey believes AI could considerably add to India's GDP growth). However, AI's power comes from extensive data collection and mining, which can encroach on individual privacy. Data privacy – broadly the principle that individuals should control how their personal data is collected, used, and shared[3] – faces novel strains from AI systems. Machine learning models may draw inferences beyond original data purposes, perform opaque "black box" profiling, and even memorize sensitive details. Thus, a core legal challenge is how to reconcile AI innovation with fundamental privacy protections[4].

This is a particularly pressing issue in India. Although India only passed a comprehensive data protection law in 2023[5], the Supreme Court has ruled that the right to privacy is a fundamental constitutional right[6]. Before 2023, privacy was monitored by sector-specific regulations. Even so, it reflected the EU's GDPR and worldwide trends, the new Digital Personal Data Protection Act (DPDP Act) does not address all AI-specific issues[7]. On the other hand, there have been no regulations that have been set up yet in the business sector and government, as they have adopted AI rapidly. The recent incident of  Delhi police using facial recognition technology

---

[2] Examining India's efforts to balance AI, data privacy | IAPP https://iapp.org/news/a/examining-indias-efforts-tobalance-ai-data-privacy
[3] What Is Data Privacy? | IBM https://www.ibm.com/think/topics/data-privacy
[4] See *K.S. Puttaswamy v. Union of India* (Right to Privacy Case), Supreme Court Observer, https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/ (last visited Sept. 3, 2025) (recognizing privacy as a fundamental right under the Indian Constitution); see also IAPP, *Examining India's Efforts to Balance AI, Data Privacy*, https://iapp.org/news/a/examining-indias-efforts-to-balanceai-data-privacy/ (last visited Sept. 3, 2025) (discussing India's struggle to reconcile AI innovation with privacy protections).
[5] See *India: Data Protection Laws of the World*, DLA Piper, https://www.dlapiperdataprotection.com/?t=law&c=IN (providing an overview of India's data protection regime); see also IAPP, *Operationalizing India's New Data Protection Law: The Challenges, Opportunities Ahead*, https://iapp.org/news/a/operationalizing-indias-new-dataprotection-law-the-challenges-opportunities-ahead/ (discussing the implementation hurdles of India's 2023 data protection law).
[6] Fundamental Right to Privacy - Supreme Court Observer https://www.scobserver.in/cases/puttaswamy-v-unionof-india-fundamental-right-to-privacy-case-background/
[7] ijbmi.org https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf

during protests has been brought into light by the difference or bias between the effective surveillance tools and inadequate monitoring[8]. Thus, this essay explores the privacy issues of AI in India. Let us first list the important privacy threats and describe how AI systems deal with personal data. Second, we examine India's legal system, along with its legislation, regulations, policies, and constitutional rights, with proper international models. To conclude, we outline the necessary technical and legal measures required to guarantee that AI is advantageous and not at the price of human rights and privacy.

**DATA-PRIVACY AND AI CONJUNCTION**: AI fundamentally needs personal data to provide functionality. On examining training datasets, personal information such as names, medical records, location traces, etc, was found frequently; machine learning algorithms "learn."[9]. Such data may be collected from smartphones, social media, public cameras, medical databases, financial records, and Internet-of-Things devices. As IBM notes, data privacy is the idea that each person should “have control over their personal data, including the ability to decide how organizations collect, store and use their data”[10]. When AI systems aggregate data from many sources, the line between purely analytic use and intrusive profiling blurs. For example, an AI-powered health app that learns from patients’ fitness tracker data might infer someone’s genetic redispositions or lifestyle habits – information the user did not explicitly provide or anticipate being revealed[11]. AI also enables unprecedented forms of surveillance and inference. Mass deployment of AI for image analysis, voice recognition, or social media monitoring allows profiles of behavior to be built automatically. Such profiling goes beyond traditional concerns: even anonymized data can often be re-identified when fed into complex models. The U.S. Supreme Court and privacy scholars have recognized that modern technology can reveal “intimate details about individuals’ lives” from ostensibly innocuous data[12]. With AI, even seemingly digital footprints (location pings, browsing history) can be correlated to reveal health status, religious or political views, and other sensitive attributes. As

---

[8] India's use of facial recognition tech during protests causes stir | Reuters https://www.reuters.com/article/world/indias-use-of-facial-recognition-tech-during-protests-causes-stiridUSKBN20B0ZP/

[9] Examining India's efforts to balance AI, data privacy | IAPP https://iapp.org/news/a/examining-indias-efforts-tobalance-ai-data-privacy

[10] What Is Data Privacy? | IBM https://www.ibm.com/think/topics/data-privacy

[11] Examining India's efforts to balance AI, data privacy | IAPP https://iapp.org/news/a/examining-indias-efforts-tobalance-ai-data-privacy

[12] See Rahul Bharati, *The Right to Privacy in the Age of Artificial Intelligence: Challenges and Legal Frameworks* (2024), SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4908340 (analyzing how AI complicates privacy protections); see also *The Right to Be Forgotten vs. AI’s Infinite Memory: A Regulatory Dilemma*, DPO India, https://www.dpo-india.com/Blogs/right-to-forgot/ (exploring regulatory challenges of applying the right to be forgotten in the AI context).

one analysis explains, the "more, the merrier" mantra of AI's need for large datasets triggers significant privacy challenges when an individual's data is used to train or refine models[13]. Equally significant, openness and control are compromised by AI's opacity, or "black box" nature. It is hard to understand the algorithm of AI on which basis it approves a loan or identifies a person as a threat. Due to this lack of transparency on the use of personal data, people find it untrustworthy. There have been instances where the AI-driven recruitment tools, in certain cases, have learned to be biased by training data and screened out women or minorities without clear logic. Without legal requirements, people cannot challenge this one-sided decision of the AI's algorithm. In this sense, AI extends beyond simple data leaks; it can embed personal information into future inferences in ways that are hard to unwind. To briefly explain this, AI worsen several traditional privacy risks, like profiling (making sensitive assumptions), data misuse (using data for surveillance or secondary analysis), data intrusion (collecting more personal data than necessary), and autonomy erosion (lack of transparency). AI also brings up new issues around data deletion and ownership. Such issues have a tremendous resonance in India. Once data are used to train a model, can they truly be "forgotten" if the model has integrated patterns from them? This tension is illustrated by debates over the "right to be forgotten" in AI's age: if a generative AI model like ChatGPT absorbs vast texts (including personal data), can an individual later demand removal of that data from the model? Experts note that "[t]his challenge becomes even more pronounced with the rise of generative AI" because "AI systems might indefinitely store or replicate personal data", making deletion orders legally and technically difficult[14]. India generates enormous amounts of personal data due to its large population and expanding digital economy.[15] At the same time, privacy law is still nascent. The Supreme Court has affirmed that informational self-determination is part of the right to life under Article 21[16], but until very recently, India lacked a comprehensive data privacy statute. The previous patchwork of rules (IT Act 2000 and the 2011 privacy rules) provided only limited protection[17]. In practice, many AI initiatives have proceeded under little regulatory scrutiny. For instance, controversy arose when police

---

[13] Examining India's efforts to balance AI, data privacy | IAPP https://iapp.org/news/a/examining-indias-efforts-tobalance-ai-data-privacy

[14] The Right to Be Forgotten vs. AI's Infinite Memory: A Regulatory Dilemma https://www.dpoindia.com/Blogs/right-to-forgot/

[15] Niranjan Sahoo, *India's Growing Digital Economy and Data Protection Challenges*, Brookings Inst. (July 31, 2023), https://www.brookings.edu/articles/indias-growing-digital-economy-and-data-protection-challenges/

[16] Fundamental Right to Privacy - Supreme Court Observer https://www.scobserver.in/cases/puttaswamy-v-unionof-india-fundamental-right-to-privacy-case-background/

[17] Data protection laws in India - Data Protection Laws of the World https://www.dlapiperdataprotection.com/?t=law&c=IN

used facial recognition during Delhi protests, prompting activists to hide their faces in masks and demand "we need to protect ourselves" from unregulated surveillance[18]. Civil society groups explicitly called for "clear rules" and algorithmic audits for law enforcement's AI use[19]. Such examples illustrate the AI–privacy nexus: the same technology enabling public safety can also threaten individual rights when unchecked.

## KEY PRIVACY CHALLENGES OF AI

AI systems create a chain of cohesive privacy challenges. A few among them are:

**Mass surveillance and profiling:** Monitoring a large number of people has been made easy by AI. In public places, computer vision and biometrics can identify and track individuals. For example, Hyderabad police and Delhi police are using such a method for facial recognition

and identifying protestors and suspects[20]. Without strict rules, this can affect the anonymity and chill free speech. As Reuters reported, Indian activists at protests fear "what they are going to do with my data," which makes the public anxious over the not-so-transparent surveillance[21]. This extends to online profiling as well: AI algorithms on social media can analyse the likes, follows, and posts, which in turn can alter their personal character. These profiles, if misused, can lead to discriminatory targeting or manipulation. India currently struggles with explicit legal limits on algorithmic profiling beyond basic consent requirements, which raises questions on how to regulate this invasive analytics.

- **Data breaches and security:** AI systems analyse sensitive data in one place, like data lakes. A breach of an AI training database could expose huge amounts of personal records. The concentration of data also makes AI infrastructure a tempting target for hackers.[22] Moreover, AI tools themselves can be exploited: by feeding in manipulative data to the system and can get data from the AI itself without it knowing that it had leaked data. For

[18] India's use of facial recognition tech during protests causes stir | Reuters https://www.reuters.com/article/world/indias-use-of-facial-recognition-tech-during-protests-causes-stiridUSKBN20B0ZP/
[19] Ibid.
[20] India's use of facial recognition tech during protests causes stir | Reuters https://www.reuters.com/article/world/indias-use-of-facial-recognition-tech-during-protests-causes-stiridUSKBN20B0ZP/
[21] Ibid.
[22] See *Securing generative AI starts with sustainable data centers*, VentureBeat (citing Gartner data showing 41 % of enterprises experienced AI-related privacy breaches and 25 % faced malicious attacks targeting AI infrastructure), https://venturebeat.com/

instance, generative models have been shown to sometimes reproduce voice-to-text content or personal details from their training set. Such vulnerabilities enforce the need for strong data security. The DPDP Act and IT Act do impose "reasonable security practices," but experts warn these are just mandatory requirements. In short, stronger technical protections like encryption, anonymisation and breach-notification laws are very important in this AI era.

- **Consent and data inference:** A privacy law is traditionally built in such a way that it produces a notice to the user and gets their consent, but AI tests this method. Users usually grant consent or only one purpose, say, a service's operation, but AI systems can add new information to the old data, projecting that it got all consent from the user. Kshitij Malhotra observes that

  India's data laws exempt "publicly available" data from protection[23], which some interpret as allowing web scraping of social media or blogs. However, when this scraped data is fed into AI, users whose data was made "public" might not expect their personal posts to train a chatbot. The result is a regulatory grey zone: data collected in one context ends up powering an unrelated AI service without fresh consent. Even where consent is obtained, fully informing users about complex AI processing is difficult. To summarise AI can undermine any consent from the user, which is a core tenet of data privacy.

- **Algorithmic bias and discrimination:** AI systems use historical data for information, and if they learns about social bias(racial, gender, caste, etc.), they may add it to their selection criteria for, let's say, a job application, and it could increase such biases. The Indian Constitution guarantees equality (Article 14) and non-discrimination (Articles 15–16); such principles must be informed in AI deployment. Analysts warn that untrained AI can reboot existing inequalities.[24] For example, an AI recruitment tool trained on past hiring data may favour certain communities over others, affecting equal opportunity norms. These concerns have legal dimensions: discriminatory outputs could violate rights without a clear remedy. The high court in K.S. Puttaswamy established that privacy is linked to

[23] To Train or Not to Train: AI and the Data Privacy Dilemma https://www.ijlt.in/post/to-train-or-not-to-train-aiand-the-data-privacy-dilemma
[24] International Monetary Fund, *IMF Warns of 'Profound Concerns' over Rising Inequality from AI*, *Fin. Times* (June 17, 2024) (reporting that generative AI "raises profound concerns about … rising inequality"), https://www.ft.com/

dignity[25]; similarly, unchecked bias in AI could undermine both privacy and equality. The **Information Technology Act** and **DPDP Act** do not explicitly ban algorithmic discrimination, nor require bias audits[26]. Thus, communities could be adversely affected by invisible automated decisions without recourse, which is a major regulatory gap.

- **Right to erasure and "infinite memory" of AI:** A right to erasure or deletion (the "right to be forgotten") is frequently included in contemporary data protection regulations. However, AI complicates this right. Once data are ingested into a model, tracing and removing all instances of that data is technically challenging. As one data protection blog warns, AI's embedding of personal data makes it "often impossible to isolate and erase specific data influences once training is complete"[27]. In the context of AI, an individual may request the removal of personal data, but the AI model itself might retain patterns derived from that data. This raises enforcement issues: can a data controller ever fully comply with an erasure request when it has built an AI model? The ongoing Indian litigation involving OpenAI's ChatGPT illustrates this dilemma. OpenAI was sued by an Indian news agency (ANI) for allegedly stealing their content without authorization; OpenAI contended that U.S. law requires it to preserve training data during litigation[28]. While that case is pitched as a copyright suit, it underscores that once data enters AI systems, companies claim they cannot easily delete it. In short, generative AI's "infinite memory" challenges traditional data deletion rights.

- **Opaque decision-making ("black box"):** AI models, particularly deep learning, are often not interpretable. Users do not know why a given decision was made. This opacity conflicts with legal norms of transparency and accountability. Courts rely on knowing the reasoning behind administrative actions; if an AI system is used in a public decision, stakeholders may demand an explanation. NITI Aayog's AI Strategy expressly warns of the "Black Box Phenomenon," emphasizing the need for explainability[29]. Without such transparency, it is difficult to ensure that data use complies with the purpose limitation or to detect if personal data is being processed unlawfully. Proposed EU regulations (the AI

[25] Fundamental Right to Privacy - Supreme Court Observer https://www.scobserver.in/cases/puttaswamy-v-unionof-india-fundamental-right-to-privacy-case-background/
[26] ijbmi.org https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf
[27] The Right to Be Forgotten vs. AI's Infinite Memory: A Regulatory Dilemma https://www.dpoindia.com/Blogs/right-to-forgot/
[28] Exclusive: OpenAI tells India court ChatGPT data removal will breach US legal obligations | Reuters
[29] National Strategy for Artificial Intelligence https://www.niti.gov.in/sites/default/files/2023-03/NationalStrategy-for-Artificial-Intelligence.pdf

Act and GDPR) aim to mandate impact assessments for high-risk AI; India's DPDP Act lacks an explicit requirement for Data Protection Impact Assessments (DPIAs) in an AI context. IAPP commentators suggest organizations should voluntarily perform DPIAs and embed privacy measures (like differential privacy or federated learning) when deploying AI[30]. Embedding these principles in law would help align AI with privacy rights.

- Data ownership and control: A less-spoken issue is who "owns" data which was once used by an AI. If an AI generates new outputs from inputs like a portrait painted by an artist, does the artist have rights over the output? And who is responsible if an AI leaks personal data? Indian law does not yet address such questions. The ANI v. OpenAI lawsuit indirectly touches on data control: ANI seeks deletion of its content used in training, while OpenAI claims legal obligation to preserve that data[31]. These disputes highlight the unsettled legal terrain: India will likely need guidance on cross-border data flows (since many AI servers are overseas) and on establishing data principals' control under its laws[32].

In summary, AI intersects with privacy at multiple levels. It magnifies classic data protection issues and introduces novel ones (like model opacity and irreversible ingestion). From a rights perspective, individual autonomy over personal data (a component of Article 21) can be threatened if AI systems consume and act on data without sufficient oversight or user agency[33]. The challenge is to craft legal guidelines that provide a solution to these risks while still allowing beneficial AI innovation. The next section surveys how India has begun to regulate this space.

## INDIA'S LEGAL AND POLICY FRAMEWORK

### CONSTITUTIONAL AND JUDICIAL FOUNDATIONS

India's journey toward privacy protection reached to an end in the 2017 Supreme Court decision in Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India[34]. In that landmark case, a nine-judge bench unanimously said that the right to privacy is basic to the right to life and

[30] Examining India's efforts to balance AI, data privacy | IAPP https://iapp.org/news/a/examining-indias-efforts-tobalance-ai-data-privacy

[31] Exclusive: OpenAI tells India court ChatGPT data removal will breach US legal obligations | Reuters

[32] Operationalizing India's new data protection law: The challenges, opportunities ahead | IAPP

[33] Fundamental Right to Privacy - Supreme Court Observer https://www.scobserver.in/cases/puttaswamy-v-unionof-india-fundamental-right-to-privacy-case-background/

[34] *Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India*, (2017) 10 S.C.C. 1 (India).

personal liberty under Article 21 of the Constitution[35]. This made informational privacy a fundamental right, overruling earlier rulings that had left privacy unprotected. The court emphasized that privacy safeguards autonomy and dignity, core values in India's constitutional scheme. Puttaswamy did not provide a comprehensive AI-specific framework; however, by recognizing privacy as a constitutional right, it established a foundation for subsequent examination of data practices. Subsequent cases, including Navtej Johar and Joseph Shine, have cited Puttaswamy to reinforce privacy in various contexts. Puttaswamy case concentrated on state action, yet it also shapes anticipations for private entities. The Aadhaar case, which came after Puttaswamy, added more details. In K.S. Puttaswamy v. Union of India (Aadhaar), the Court said that Aadhaar was valid but put strict rules in place to protect privacy (proportionality, limited use, no comprehensive profiling). The three judges who made up the majority said again that even "reasonable surveillance" must be balanced against constitutional safeguards. These decisions suggest that any AI-driven data practice (especially by the government) would undergo strict privacy justification. A future litigant could potentially challenge state AI surveillance schemes under Article 21.

## STATUTORY DATA PROTECTION REGIME

India lacked a dedicated data protection law until recently. The Information Technology Act, 2000 (IT Act) and associated rules provided the closest information. Under the IT Act, Section 72A penalized breaches of computer data, and Section 43A enabled compensation for negligent data protection (though these were rarely invoked). The IT (Reasonable Security Practices) Rules, 2011, defined "sensitive personal data or information" and required entities to implement reasonable safeguards for it. However, this regime was weak by global standards: many classes of personal data fell outside the "sensitive" scope, and enforcement was minimal[36]. Nevertheless, it laid a foundation: India recognised the principle of lawful and secure data handling, albeit in a limited way. India finally enacted its first comprehensive data protection law in 2023: the Digital Personal Data Protection Act, 2023 (DPDP Act). This Act (often called the DPDPA) was passed by Parliament on August 11, 2023 and published in the Gazette[37]. It broadly models itself on the EU's GDPR: imposing principles like consent, purpose limitation, data minimization, and data subject rights (access, correction, erasure,

[35] Fundamental Right to Privacy - Supreme Court Observer https://www.scobserver.in/cases/puttaswamy-v-unionof-india-fundamental-right-to-privacy-case-background/
[36] Data protection laws in India - Data Protection Laws of the World https://www.dlapiperdataprotection.com/?t=law&c=IN

etc.)[37]. Data fiduciaries (analogous to controllers) must process data lawfully and implement security safeguards. Extraterritorially, the DPDP Act applies to foreign companies offering goods/services to Indian residents, much like GDPR's reach. According to analysts, India's DPDP establishes a "consent-oriented approach" requiring "free, specific, informed, unconditional" consent[38]. However, significant caveats remain. First, the Act currently applies only to personal data in digital form, not to offline data or non-personal data[39]. It essentially codifies that India's privacy regime concerns digital data, leaving analogue data outside its ambit. Second, key details await rules (the Act's provisions kick in when notified and rules are framed). The rules were still in draft form, so the law is not fully operational yet as of late 2024[40]. Third, experts say that the DPDP Act does not openly address AI-specific challenges.[41] It lacks any requirement for Data Protection Impact Assessments tailored to AI, and it does not impose algorithmic transparency obligations[42]. For example, the IJBMI analysis observes that the DPDP Act "introduces the concept of consent-based data usage" but "lacks clear and unambiguous provisions for regulating and checking algorithmic bias or automated decision-making"[45]. In short, while the DPDP Act raises the baseline for data privacy in India, it remains largely a general framework. It does not automatically solve the "AI problem" – those specifics will likely need new rules or separate legislation.

---

[37] Operationalizing India's new data protection law: The challenges, opportunities ahead | IAPP
[38] Ibid.
[37] See *India: Data Protection Laws of the World*, DLA Piper, https://www.dlapiperdataprotection.com/?t=law&c=IN (overviewing India's data protection regime); see also IAPP, *Operationalizing India's New Data Protection Law: The Challenges, Opportunities Ahead*, https://iapp.org/news/a/operationalizing-indias-new-data-protection-law-thechallenges-opportunities-ahead/ (discussing challenges and opportunities in implementing India's 2023 data protection law).
[39] Data protection laws in India - Data Protection Laws of the World https://www.dlapiperdataprotection.com/?t=law&c=IN
[40] See *India: Data Protection Laws of the World*, DLA Piper, https://www.dlapiperdataprotection.com/?t=law&c=IN (overviewing India's data protection regime); see also IAPP, *Operationalizing India's New Data Protection Law: The Challenges, Opportunities Ahead*, https://iapp.org/news/a/operationalizing-indias-new-data-protection-law-thechallenges-opportunities-ahead/ (discussing challenges and opportunities in implementing India's 2023 data protection law).
[41] See Janhvi Singh, *AI Diffusion on India's Data Protection Policy* (Feb. 16, 2025) (noting that although the DPDP Act, 2023 provides a legal framework for personal data, *"it does not adequately address AI-specific risks such as bias in automated decision-making, lack of transparency in AI-driven processes, and challenges in enforcing data minimisation"*)
[42] See *Artificial Intelligence and Data Privacy in India*, *Int'l J. of Bus. & Mgmt. Invention*, Vol. 14, Issue 8, at 6–10, https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf (discussing challenges of AI and privacy protection in India); see also *AI and Data Privacy: Creating a Robust Legal Framework in India*, WithLaw (2023), https://withlaw.co/blog/Technology-and-Innovation-1/AI-and-Data-Privacy:-Creating-a-Robust-Legal-Frameworkin-India (analyzing legal frameworks for AI governance in India).

Complementing the DPDP Act is the IT Act's continued authority over certain cyber matters. Sections 43A and 72A of the IT Act still allow citizens to sue for negligence or unauthorised disclosure of personal data. Section 66E criminalises the violation of privacy by capturing images. The recently introduced (but not yet passed) Digital India Act, 2023, aims to overhaul the IT Act and does propose AI-related provisions (for example, algorithmic impact assessments and deepfake regulations)[43]. Additionally, sectoral laws and regulations may apply. For instance, the Reserve Bank of India requires banks to protect customer data, and the Reserve Bank (RBI) has even set up a policy for "Disclosures by NBFCs" including privacy norms. Financial firms, healthcare providers, telecoms, and other regulated sectors have their own data guidelines. Some notifications (like a proposed Digital Personal Data Protection (DPDP) Rule) envisage carve-outs or obligations for AI data use.

**SPECIFIC AI-FOCUSED GUIDELINES AND POLICIES**

Though India lacks a singular "AI Act," the government has issued several policy documents and guidelines on AI. In 2018, NITI Aayog released a National Strategy for Artificial Intelligence ("AI for All")[44]. That strategy emphasizes ethical AI, including fairness, accountability and privacy, and envisions leveraging AI for inclusive growth (in healthcare, agriculture, education). It explicitly notes that data should be used "ethically" and calls for standards on privacy and bias[45]. Later, the government framed Principles for Responsible AI (2021), which outlines values like impartiality, transparency and privacy. These principles are not legally binding, but this shows India's normative stance.

Regulatory guidance has occurred recently. In 2024, India's Ministry of Electronics and IT (MeitY) issued Model Guidelines for AI through a draft "Indian Standard" and government committee recommendations. These draft guidelines would require government entities to conduct "Algorithmic Impact Assessments" before deploying high-risk AI systems in public administration. They also mandate centralized AI auditing mechanisms and stress data anonymization. Although not yet law, they could influence how agencies use AI. Similarly, MeitY has indicated that any AI system likely to affect elections, public health, or personal

[43] Ibid.
[44] ijbmi.org https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf
[45] National Strategy for Artificial Intelligence https://www.niti.gov.in/sites/default/files/2023-03/NationalStrategy-for-Artificial-Intelligence.pdf

data will need prior approval[46].

Institutionally, India is considering new bodies. The DPDP Act creates a Data Protection Board of India to adjudicate privacy complaints. There is also talk of establishing an AI Standards Body (some recommend adapting the Bureau of Indian Standards). However, enforcement capacity remains weak. As commentators note, even with data laws, there is “a complete lack of comprehensive AI-specific law”, and no existing statute mandates algorithmic audits or bias protocols[47]. Enforcement agencies (like MeitY, RBI, TRAI) currently do not have explicit AI specific mandates. The legal response is thus a patchwork: existing data protection and IT laws cover some aspects of AI, new policies set expectations, but much is left undefined.

## COMPARISONS WITH INTERNATIONAL FRAMEWORKS

Globally, jurisdictions are controlling AI privacy. The European Union recently passed the AI Act, classifying AI applications by risk and requiring transparency, bias testing, and human oversight for high-risk systems. It also adds GDPR’s strong data protection rules with AI-specific duties.

The U.S. has a fragmented approach, with sectoral privacy laws only on health, finance. And proposed bills, but no federal AI law yet. China has strict data localization and security laws and has begun requiring AI model registration.

India’s new DPDP Act is broadly similar to GDPR in form (requiring consent, data minimization, breach notification, and protection impact assessments generally[48]). However, GDPR’s Article 22 grants a “right to explanation” against solely automated decisions – India has no direct analogue. The EU also explicitly treats biometric and genetic data as “special”, requiring extra safeguards. India’s concept of Sensitive Personal Data in the old rules (IT Act 2011) was narrow and has been shelved in the DPDP Act (which uses a broad “data fiduciary” concept).[52] On AI specifically, the EU AI Act would impose explicit bans (e.g. predictive

[46] ijbmi.org https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf

[47] ijbmi.org https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf

[48] See IAPP, *Operationalizing India’s New Data Protection Law: The Challenges, Opportunities Ahead*, https://iapp.org/news/a/operationalizing-indias-new-data-protection-law-the-challenges-opportunities-ahead (discussing implementation challenges of India’s 2023 data protection law); see also *Artificial Intelligence and Data Privacy in India*, *Int’l J. of Bus. & Mgmt. Invention*, Vol. 14, Issue 8, at 6–10, https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf (examining AI and privacy protection in the Indian context).

policing based on sensitive data) and duties (AI transparency). India has not yet banned any AI use cases, though a proposed law might forbid automated profiling of sensitive traits or require people's opt-in for certain AI uses.

The EU's GDPR and AI Act offer benchmarks for India. For example, data protection authorities in Europe can audit algorithms and issue heavy fines. Indian regulators could look to GDPR's privacy-by-design and purpose limitation doctrines to adapt to AI. Moreover, cross-border data flow rules in GDPR ensure EU citizens' data gets protection even abroad. India's DPDP Act similarly intends to regulate foreign entities processing Indians' data[49], which is crucial given that many AI platforms (OpenAI, Google, etc.) are global. However, differences remain: India's approach so far appears more permissive on data use (e.g. allowing "publicly available" data) and less focused on strict rights. Legal scholars argue that wholesale adoption of EU-style rules may not fit India's development needs, but the principles of fairness and accountability certainly inform the debate[50].

**ONGOING DEBATES AND PROPOSALS**

Legal and academic commentators in India are actively debating how to update the framework. Some argue for an independent AI-specific statute or at least AI amendments in the Digital India Act. Others believe existing laws can be tweaked (for example, by issuing detailed AI rules under the DPDP Act, or strengthening sectoral laws). A Carnegie Endowment study notes that, unlike the EU or China, India has been hesitant to impose a rigid AI regulatory regime; regulators tend to prefer guidelines and industry self-regulation for now[51]. Businessists and technologists warn that over-regulation could stop innovation. On the other hand, civil society stresses the need to protect marginalized groups from discrimination and surveillance.

Critically, there is an equillibrium that any approach must balance innovation with rights. The fundamental ideas of necessity, proportionality, accountability, and transparency are emphasized by legal scholars. For instance, there should be minimal intrusion and a clear public interest in any AI surveillance or profiling. In a similar vein, people should be informed

49 Operationalizing India's new data protection law: The challenges, opportunities ahead | IAPP https://iapp.org/news/a/operationalizing-india-s-new-data-protection-law-the-challenges-opportunities-ahead
50 WHY WE NEED DATA PROTECTION LAWS FOR AI IN INDIA https://defactolawjournal.org/papers/why-we-needdata-protection-laws-for-ai-in-india/
51 India's Advance on AI Regulation | Carnegie Endowment for International Peace https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en

when their personal data is processed so they can challenge decisions. The government has shown that it is receptive to feedback from a variety of stakeholders by sharing draft AI guidelines and DPDP Act rules for public comment.

**REGULATORY AND TECHNICAL PROTECTIONS**

A combination of legislative regulations and technological solutions will be needed to resolve AIprivacy conflicts. Legally speaking, India could fortify its system by:

● Requiring Privacy Impact Assessments (PIAs): a formal evaluation should be carried out to guarantee that any AI system handling personal data faces privacy risks (as the GDPR/AI Act do). A PIA requires identifying what data is used, potential harms, and solutions. This is partly anticipated in draft DPDP rules (which mention DPIAs for large data processing), but should explicitly cover AI projects.

● Algorithmic transparency and audits: AI systems that use governmental and high-stakes information must disclose basic information about their operation could be important. For example, requiring a government agency to publicly explain the criteria used by an algorithmic decision tool. Even if the ownership details remain hidden, mandating independent audits (possibly by the Data Protection Board or a new AI audit authority) would increase accountability. The proposed Digital India Act envisions "algorithmic audits" for deepfakes and AI[52], a model India could extend to other contexts.

● Stronger consent and control mechanisms: The DPDP Act's approach is consent-centred, but India's pro-AI position has initially allowed wide usage of "public" data[53]. Regulators could clarify what use of publicly available data is permissible for AI training. For instance, requiring even aggregated, anonymized data gathering to respect certain boundaries, or enforcing that AI firms honor takedown requests for specific content.New ideas for consent frameworks, such as MeitY's idea of "consent managers" to handle granular consents, could give people more control over how their data is used in AI platforms[54].

● Security and Privacy by Design Standards: The IAPP says that companies should use

[52] ijbmi.org https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf
[53] To Train or Not to Train: AI and the Data Privacy Dilemma https://www.ijlt.in/post/to-train-or-not-to-train-aiand-the-data-privacy-dilemma
[54] Operationalizing India's new data protection law: The challenges, opportunities ahead | IAPP

"privacy by design" methods when making AI[55]. This means collecting only the data you need and using encryption or other technologies that protect privacy. For example, adding statistical noise to data can help train a model without giving away individual data. Federated learning is another way to do this. In this method, models are trained on devices and only the necessary updates are shared. The law might make these kinds of methods necessary or even encourage them for sensitive situations. The NITI Aayog report clearly asked for "advanced anonymization protocols" and higher privacy standards in AI tools[56].

● Fairness and Anti-Discrimination Measures: There could be legal protections against bias. India's Constitution already guarantees equality, but procedural remedies could be added, like giving people a way to sue if an AI-driven decision violates their fundamental rights. Data protection law could clearly say that processing sensitive personal data for profiling is against the law (like GDPR's rules about sensitive categories). Before deployment, regulatory guidelines may require representative training data or bias testing. Some jurisdictions (e.g. the EU) are looking at granting a “right to explanation” or “human-in-the-loop” for important decisions; India could consider analogous safeguards via DPDP rules or sector regulations.

● Enforcement and redress: Ensuring compliance is as important as enacting rules. The Data Protection Board, once constituted, will need expertise to handle complex AI cases. Sector regulators like RBI for finance, SEBI for securities, and TRAI for telecom should incorporate AI risk oversight in their mandates. Privacy complaints must be resolvable; victims of AI errors should have access to appeal and compensation.

On the technical front, collaboration between policymakers and technologists is key. Standardized bodies like the BIS or IITs can develop norms for AI data use. India might also join international efforts on AI ethics. Teaching judges and government workers about AI will help them enforce the rules in a smart way. Last but not least, people need to know about their privacy rights and how AI systems use their data. For example, if police use facial recognition, the public should be informed and have a chance to talk about it. The Reuters report on the protests in Delhi shows that not being transparent makes people distrustful[57].

---

[55] Examining India's efforts to balance AI, data privacy | IAPP
[56] National Strategy for Artificial Intelligence
https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
[57] India's use of facial recognition tech during protests causes stir | Reuters

## CONCLUSION

Artificial Intelligence promises transformative benefits, but it also poses unforeseen challenges to data privacy. Due to its design, AI thrives on analyzing personal data to create patterns – a process that can easily disrupt individual autonomy and dignity. In India, the right to privacy is now

constitutionally enshrined[58] and the nation has finally created a general data protection law[59], but the specific legal treatment of AI remains a work in progress. Today's statutes focus mainly on consensual data processing and security, without fully grappling with AI's "black box" and biased nature[60]. Case law gives broad rights (courts have voided illegal surveillance), but procedural data rights (like erasure) face practical limits with AI.[61]

India needs to create a comprehensive framework that establishes clear privacy standards for AI systems. This could mean changing global best practices, like the GDPR's rules for privacy impact assessments and transparency, and making rules just for AI. At the same time, regulators should properly stop useful AI innovation, especially in important areas like health care and education. It is important to have a balanced approach that is based on constitutional values and human rights. AI governance cannot depend solely on technology. To build trust, there needs to be strict laws, careful enforcement, and an educated public. As one analysis notes, "it is extremely important that we set much higher standards for privacy and protection in case of AI tools"[62]. India's policymakers must pay attention this call. By making privacy a priority from the start, holding people accountable, and protecting consent, India can use AI to its fullest while still protecting the privacy and freedom of its people. The Constitution says that protecting personal liberty requires no less.

---

[58] Fundamental Right to Privacy - Supreme Court Observer https://www.scobserver.in/cases/puttaswamy-v-unionof-india-fundamental-right-to-privacy-case-background/

[59] Data protection laws in India - Data Protection Laws of the World https://www.dlapiperdataprotection.com/?t=law&c=IN

[60] ijbmi.org https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf

[61] See *The Right to Be Forgotten vs. AI's Infinite Memory: A Regulatory Dilemma*, DPO India, https://www.dpoindia.com/Blogs/right-to-forgot/ (analyzing regulatory challenges of applying the right to be forgotten in the AI era); see also *Artificial Intelligence and Data Privacy in India*, *Int'l J. of Bus. & Mgmt. Invention*, Vol. 14, Issue 8, at 6–10, https://www.ijbmi.org/papers/Vol(14)8/14080610.pdf (examining AI and privacy protection in the Indian context).

[62] National Strategy for Artificial Intelligence https://www.niti.gov.in/sites/default/files/2023-03/NationalStrategy-for-Artificial-Intelligence.pdf

**References:**

1. *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1
2. Digital Personal Data Protection Act, 2023
3. Academic analyses of AI/privacy (e.g. Bharati, *The Right to Privacy in the Age of AI*, SSRN 2024)
4. Government strategy documents (NITI Aayog, 2018)
5. International Association of Privacy Professionals (IAPP) commentary
6. Investigative journalism (e.g. Reuters on India's use of facial recognition).