ISSN (O): 2584-2196

INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND EXPLORATION

Volume 3 | Issue 6

2025

Website: www.ijlae.com

Email: editor@ijlae.com

ISSN (O): 2584-2196

AI AND PRIVACY RIGHTS IN INDIA

Reshma Rajan

4th Year, Law Student, Christ Academy Institute of Law.

ABSTRACT

India is experiencing rapid growth in Artificial intelligence (AI) adoption and innovation. This rush is driven by a large tech-savvy workforce, expanding digital infrastructure, and government initiatives like Digital India. However, this AI revolution is unfolding against a backdrop of evolving privacy regulations and growing public awareness of data protection issues. The Indian government has recognized both the potential of AI and the need for privacy safeguards. The National Strategy for AI, launched in 2018, aims to position India as an AI powerhouse. At the same time, the proposed Personal Data Protection Bill, inspired partly by the EU's GDPR, seeks to establish a comprehensive framework for data privacy. Indian AI start-ups and tech giants are increasingly focusing on privacy-preserving AI techniques. Efforts include developing federated learning systems for healthcare applications, implementing differential privacy in financial services, and exploring secure multi-stakeholder computation for collaborative AI projects across organizations. Several challenges persist in balancing AI innovation with privacy protection in India. These include a fragmented regulatory landscape, limited public understanding of AI and privacy issues, and the need for massive datasets to train AI models effectively while respecting individual privacy rights. India's unique context, including its diverse population and varying levels of digital literacy, necessitates tailored approaches to privacy-preserving AI. Innovations in this space include vernacular language AI models trained on synthetic data and block chain-based consent management systems for data sharing. As a way ahead, more focus is needed in strengthening the legal and ethical framework for AI development and deployment. Investing in research on privacy-enhancing technologies suitable for India's context. Encouraging public-private partnerships to develop privacy-respecting AI solutions for social good is a good option. Enhancing digital literacy and awareness about AI and privacy rights remains a viable instrument. As India continues its AI journey, striking the right balance between innovation and privacy protection will be crucial for sustainable and responsible AI growth in the country. This will truly bolster India's AI governance and make it a vibrant AI ecosystem.

ISSN (O): 2584-2196

Keywords: Artificial Intelligence, Privacy, Models, Ecosystem, Innovation, India

INTRODUCTION

The Artificial intelligence (AI) has been developing since ages and has been a vital part of all of our lives. The evolution of technology from social media to healthcare has been developed rapidly. Due to the evolution of technology, there have been more opportunities for economic as well as societal growth. “Data is often considered the new oil, a vital resource that fuels AI algorithms and models. However, unlike oil, data pertains to individuals' personal lives, and its misuse can lead to severe privacy violations and breaches of trust.”[1] Due the swift advancement of AI they are has been various challenges like privacy concerns among individuals. This makes incorporating privacy concerns not only a legal necessity but also as moral necessity. As Artificial intelligence is increasingly integrated into everyday life, they generate and rely on large amounts of personal data, posing serious concerns around data protection, consent and privacy. The balance between leveraging AI for societal progress and safeguarding individual rights is becoming significant component of modern governance.

India’s artificial intelligence market was valued at about USD 6.8 billion in 2024, and it is expected to reach USD 27.7 billion by 2032. This growth represents a compound annual growth rate (CAGR) of 19.2% from 2025 to 2032[2]. The strong expansion is driven by more industries adopting AI, government initiatives like the National AI Strategy, and a rapidly growing AI startup scene. At the same time, there is rising public concern about data privacy. A Rcent study and research shows that 65% of Indian internet users worry about how AI applications manage their personal data

The initiatives undertaken by the Indian government like the National Strategy for AI and the protection Bill also highlight the challenges of creating a cohesive regulatory framework for rapid evolution of technology. AI in India is still in its formative stage offering a lot of opportunities to shape a framework that respects individual privacy rights while developing advancements of AI. This research paper seeks to analyse the current landscape of AI adoption in India and identify challenges

[1] Available at: https://www.gmiresearch.com/report/india-ai-market/

in implementing privacy preserving rights. Finally, the study proposes ethical frameworks surrounding AI development to ensure privacy protection in India

The problem of this study is due to the swift evolution of AI in India. This rapid evolution is driving innovation and developing industries. However, this development comes with disruptive challenges like privacy concerns as AI always rely on personal information for functioning. India confronts dual challenges that are development of promotion of AI as well as guaranteeing strong data privacy. Despite of initiatives like personal data protection and the National strategy for AI, there are gaps in regulatory framework, limited public awareness and effective implementation. This research aims to address the on how to achieve a balance between AI advancement and privacy rights. This study proceeds with an assumption that it's on through a robust legal framework, increased public awareness and effective implementation of privacy-preserving technologies can enhance individual privacy rights while fostering AI innovation in India.

Dev Kaur explores the right to privacy as a fundamental human right recognized globally.[3] This study highlights the landmark Supreme Court judgment in Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017),[4] which established privacy as a constitutional right under Article 21 of the Indian Constitution. The judgment has catalyzed legislative reforms aimed at protecting personal data in cyberspace, notably through the Personal Data Protection Bill, 2019. It indicates that it has made strides in recognizing privacy rights, challenges remain due to a fragmented regulatory framework and limited public awareness of data protection issues.

Dr. Esha Chatterjee, examines the social implications of AI among 50 individuals aged 18-45 using a mixed-methodology approach. The findings reveal frequent AI usage for tasks like household management and digital interactions, enhancing productivity but also raising privacy issues due to extensive data sharing by the individuals.[5]

The thematic report by the Centre for Communication Governance at National Law University Delhi emphasizes that while AI can offer social benefits, it also poses risk such as discrimination against

[3] Dev Kaur, *"A Comparative Study of the Evaluation on the Right to Privacy in India and the UK, Their Legal Frameworks and Judicial Interpretation" (2024)*
[4] Justice K.S Puttaswamy (Retd.) v. Union of India, (2017) 6 MLJ 267; (2017) 10 SCC 1, available at https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors
[5] *Dr. Esha Chatterjee's study, "Examining the Impact of AI on Daily Life through Usage Patterns, Privacy Concerns and Social Dynamics" (2024)*

marginalised communities and violations of privacy.[6] Concerns arise regarding existing data protection frameworks, particularly their ability to address the challenges posed by AI, including the re-identification of anonymized data. The proposed Personal Data Protection Bill aims to create a comprehensive legal framework, but scholars argue that a unified regulatory approach is essential to effectively govern AI technologies across sectors.

Amlan Mohanty and Shatakratu Sahu looks deeply into the current state and future prospects of AI regulation in India. Their study[7] evaluates diverse perspectives from government, industry, and civil society stakeholders, highlighting India's oscillation between a pro-innovation and cautious regulatory approach. The authors emphasize the need for targeted policies, discussing government initiatives like the Digital India Act and recommendations from MeitY for high-risk AI systems. They detail global approaches to AI regulation, contrast self-regulation with binding frameworks, and call for a collaborative, risk-based strategy. Proposals include empowering sectoral regulators, strengthening state capacity, and adopting a "whole of government" approach for AI governance in India

CURRENT LADSCAPE OF AI ADOPTION IN INDIA

Artificial Intelligence (AI) is quickly changing industries around the world, and India is a key player in this tech change. AI can improve human thinking, learning, problem-solving, and decision-making. This brings new chances for economic and societal growth. India's AI strategy is broad, combining strong government programs, active participation from the private sector, and data governance systems to encourage and manage AI use safely. More than 56% of adults in cities actively use generative AI tools. This makes India the top AI adopter in the Asia-Pacific region. Notably, about 63% of Indian adults say they understand AI, which is among the highest rates globally. This knowledge is largely driven by a tech-savvy millennial population that is boosting AI literacy and job readiness[8].

A main part of India's AI infrastructure is the Digital India program, which the Ministry of Electronics and Information Technology (DeitY) launched in 2015. This ambitious program aims to digitally empower over 1.2 lakh villages by improving broadband access and

[6] The Centre for Communication Governance at National Law University Delhi. https://www.ohchr.org/Documents/Issues/DigitalAge/Submissions/CSOs/CCG.pdf

[7] Amlan Mohanty and Shatakratu Sahu, *India's Advance on AI Regulation* (2024)

[8] https://www.deccanherald.com/technology/artificial-intelligence/indias-ai-adoption-growing-at-record-pace-momentum-tripled-year-over-year-openais-oliver-jay-3789831

digitizing government services through platforms like DigiLocker. Initiatives like the Pradhan Mantri Gramin Digital Saksharta Abhiyaan (PMDISHA) promote digital skills in rural areas. The National Policy on Electronics offers a roadmap for the electronics sector. Other programs, such as the Arogya Setu app, focus on public health. Major events like the G20 and India AI Summit highlight India's dedication to building a safe AI ecosystem with strong infrastructure, skill development, and support for startups[9].

Supporting the digital framework is the National Data Governance Framework Program (NDGFP), led by the India Data Management Office (IDMO). NDGFP sets standards for data collection, sharing, and anonymization, creating a library of high-quality anonymized and non-personal datasets. This framework aims to boost innovation, economic growth, and lessen regional gaps by focusing on digital inclusion, ethical data use, and partnerships between public and private sectors. These efforts not only give researchers and startups important resources but also improve India's position in AI and data analytics[10].

The National Strategy for Artificial Intelligence, introduced by NITI Aayog in 2018, focuses on practical AI solutions that meet India's specific needs. Key sectors include healthcare, where AI helps with early disease detection, telemedicine, and drug discovery. Agriculture uses AI for precision farming. Education benefits from personalized learning solutions that connect urban and rural students. Banking and finance apply AI for fraud detection and predictive analysis. Public administration is also using AI for tasks like digitizing land records and improving policing and traffic systems. The BharatNet program boosts rural access by providing broadband to about 2.5 lakh gram panchayats (villages), allowing AI applications in remote areas. The government also supports AI research centers at top institutions like IITs and IISc. The SMART Cities Mission combines AI with infrastructure solutions in urban areas. Meanwhile, defense and national security advance through initiatives like SAMEER and Cyber Surakshit Bharat, and the National Supercomputing Mission provides essential computing power for extensive AI research and big data analysis[11].

[9]Available at: https://indiaai.gov.in/article/india-ai-governance-guidelines-empowering-ethical-and-responsible-ai
[10]Available at: https://www.deloitte.com/in/en/services/consulting/about/indias-dpdp-rules-2025-leading-digital-privacy-compliance.html
[11]Available at: https://www.ey.com/en_in/insights/cybersecurity/transforming-data-privacy-digital-personal-data-protection-rules-2025
https://www.ey.com/en_in/insights/cybersecurity/transforming-data-privacy-digital-personal-data-protection-rules-2025

The private sector's uptake of AI reflects this progress. Recent studies show that 47% of Indian businesses now have several generative AI applications in use and 23% are running pilot programs. Millennials form a significant knowledge base, with 63% of adults in urban areas claiming a strong grasp of AI concepts, which is much higher than their peers in Singapore and Australia. Companies are investing heavily—over US$31 million annually—in AI technology, anticipating returns within three years according to 93% of businesses. These investments cover software, infrastructure, talent development, and consulting, driving India's AI progress and optimism about its economic benefits[12].

At the data governance level, the India Datasets Program promotes AI innovation by providing high-quality, controlled, non-personal datasets for research and development. The India Data Management Office ensures secure and responsible data management, building trust and cooperation among government agencies, private entities, and researchers. Together, these efforts highlight India's strategy to balance quick AI adoption with responsible practices and data privacy, ensuring inclusive and sustainable technological progress[13].

CHALLENGES IN IMPLEMENTING PRIVACY-PRESERVING RIGHTS IN INDIA

India's data privacy landscape is changing significantly with the introduction of the Digital Personal Data Protection (DPDP) Rules 2025. These rules aim to consolidate various regulations into a single framework that focuses on consent, accountability, and managing breaches. However, this change brings major implementation challenges, especially for organizations dealing with shifting compliance timelines and operational difficulties. Small and medium enterprises struggle more due to limited resources needed to set up necessary technical safeguards like encryption, audit trails, and breach detection systems. Additionally, strict consent management requirements come into play, requiring clear and easily revocable

[12] Available at: https://indiaai.gov.in/news/india-leads-in-ai-adoption-says-bcg-study
[13] Available at: https://indiaai.gov.in/article/india-ai-governance-guidelines-empowering-ethical-and-responsible-ai

consent as the rules state. Businesses must redesign their systems to include these features, making compliance a complex, resource-heavy task[14]

At the same time, key technological obstacles remain. While data anonymization is crucial for privacy, the growth of advanced data analytics poses risks of re-identification. The rules require strong data protection measures, but ongoing advancements in artificial intelligence complicate the challenge of keeping data anonymous. Consent mechanisms are also under pressure, as users often struggle to understand complicated AI-driven data practices. This highlights the need for clear and accessible communication to ensure truly informed consent[15].

Public awareness and trust represent another important challenge. Despite existing legal frameworks, many data subjects lack knowledge about their privacy rights and how to enforce them. This ignorance fuels skepticism about AI and data-driven technologies and hampers the adoption of responsible AI applications. Organizations face significant compliance demands, which often overwhelm smaller companies, forcing them to invest heavily in technology, training, and policy development to meet DPDP requirements[16].

Enforcement frameworks also have notable limitations. The regulatory authority's limited resources slow down timely investigations and penalties, weakening the deterrent effect crucial for data protection. Moreover, the rapid pace of AI innovation, especially in generative models and automated decision-making, often surpasses regulatory adaptation, revealing weaknesses in privacy protections. These shortcomings require flexible regulatory responses supported by advanced technological solutions and comprehensive stakeholder involvement to build a resilient and trustworthy AI ecosystem in India[17].

India’s DPDP Rules 2025 represent a significant step towards better data protection, achieving their full potential requires tackling several challenges. These include aligning legal frameworks, advancing technology, preparing organizations, educating the public, and

[14]Available at: https://www.deloitte.com/in/en/services/consulting/about/indias-dpdp-rules-2025-leading-digital-privacy-compliance.html
[15]Available at: https://www.legal500.com/developments/thought-leadership/data-protection-laws-in-india-tackling-compliance-challenges-under-the-dpdpa-2023-draft-dpdpr-2025/
[16]Available at: https://www.drishtiias.com/daily-updates/daily-news-editorials/towards-a-robust-digital-data-protection-regime-in-india
[17]Available at: https://www.ey.com/en_in/insights/cybersecurity/transforming-data-privacy-digital-personal-data-protection-rules-2025

strengthening enforcement. A well-rounded approach is essential to balance AI-driven innovation with the need for strong privacy protection.

ILLUSTRATION

Practical incidents highlight the privacy risks that come with using AI in India. For example, a 2023 breach at a health-tech AI startup exposed thousands of patients' sensitive records, showing weaknesses in data management. Likewise, unauthorized use of facial recognition technology by law enforcement has raised questions about consent and privacy rights. This situation reveals the gap between what technology can do and the regulations that oversee it.

ETHICAL FRAMEWORKS SURROUNDING AI DEVELOPMENT TO ENSURE PRIVACY PROTECTION IN INDIA

Fast changes in AI have opened vast windows of innovation and economic growth for India. However, it also raises critical concerns over privacy protection. It is important that such credible ethical frameworks be established to ensure appropriate alignment of this technology with societal values and safeguard rights. Addressing AI's privacy challenges in India needs input from various groups. Civil society organizations actively support digital rights and conduct academic research. International partnerships, like those with the Global Partnership on AI, help put India’s regulations in line with global best practices.

India’s recent AI Governance Guidelines of 2025 represent an important move toward creating an ethical framework that balances innovation with privacy protection. These guidelines stress key principles such as transparency, accountability, fairness, and user consent, which are essential for responsible AI development. Transparency requires that AI systems explain their decision-making processes clearly. This helps stakeholders understand how data is collected, processed, and used, building trust and accountability. Accountability means that developers and organizations must take responsibility for the outcomes of their AI systems, especially to prevent privacy breaches or malicious uses. Fairness is crucial to ensure that AI systems do not reinforce biases or discriminate against marginalized groups. This calls for fair data collection practices and ongoing bias monitoring. User consent is a crucial aspect of privacy. It is strengthened through the need for clear, informed, and

revocable consent mechanisms, ensuring individuals retain control over their data even when it is used for AI training or processing[18].

Institutional mechanisms further support these principles. The guidelines suggest creating ethics committees within organizations to assess AI projects for risks related to privacy, bias, and ethical issues before deployment. The proposal includes establishing regulatory bodies to oversee AI development across sectors, making sure ethical standards are maintained through ongoing monitoring and guidance. Public consultation processes are encouraged to gather diverse stakeholder perspectives, including input from civil society, industry experts, and the general public. This approach aims to create a strong, multi-layered oversight system that encourages responsible AI innovation[19].

On the technological side, privacy-preserving tools like differential privacy, federated learning, and homomorphic encryption play a key role in the guidelines. These allow organizations to analyze data without sacrificing individual confidentiality. These techniques work alongside solid data governance practices, stressing data provenance, secure storage, and restricted access controls. The guidelines also support public awareness campaigns and training programs to teach stakeholders about AI ethics, privacy rights, and responsible data handling. Furthermore, international cooperation is highlighted as vital, with India actively participating in global standards and treaties like those organized through the Global Partnership on AI to ensure its frameworks are both globally aligned and locally effective[20].

The 2025 AI governance guidelines represent a pivotal shift toward a responsible, transparent, and inclusive AI ecosystem in India. While largely voluntary, their principles set the stage for future legislation and sector-specific regulations. This fosters an environment where technological innovation takes place within a strong ethical framework that prioritizes citizen privacy and human rights. These guidelines highlight India's commitment to responsible AI

[18]Available at: https://indiaai.gov.in/article/india-ai-governance-guidelines-empowering-ethical-and-responsible-ai
https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf

[19]Available at: https://visionias.in/blog/current-affairs/indias-new-ai-governance-guidelines-push-hands-off-approach

[20] Available at: https://www.aidataanalytics.network/data-science-ai/news-trends/india-unveils-new-ai-governance-guidelines-to-encourage-responsible-adoption

growth that reflects its constitutional values and socio-economic realities, ensuring sustainable development along with privacy protections[21].

FUTURE OUTLOOK AND RECOMMENDATIONS

Looking ahead to the next five years, India is set to improve its AI regulations and privacy structures. The goal is to balance innovation with responsibility and community protection. The Ministry of Electronics and Information Technology (MeitY) plans to release a national AI regulation draft that focuses on specific sectors and flexible governance instead of a universal law. This method encourages companies to self-regulate while also having clear rules for high-risk AI uses, like algorithmic bias and deepfakes. Improving technical infrastructure, such as providing subsidized computing resources and India-specific datasets, will help ensure fair AI development across different sectors and regions[22].

Building institutional capacity is key to this strategy. It aims to strengthen regulatory bodies, improve AI knowledge among citizens and professionals, and set up complaint processes for AI-related issues. Future regulations might include a liability framework that ties responsibilities to the risk levels of AI systems. This promotes accountability without hindering innovation. Additionally, increased focus on cross-border data management and global cooperation will help India align with international AI standards while protecting its data interests[23].

Upcoming policies should improve digital inclusion by encouraging AI adoption among micro, small, and medium enterprises through incentives and targeted funding. Principles like transparency, fairness, and privacy by design are likely to be more integrated into the development processes, backed by strong public consultations to engage society. The changing AI landscape might also lead to updates in the Digital Personal Data Protection Act, possibly requiring AI audits, privacy assessments, and easier ways for citizens to seek help[24].

---

[21] Available at: https://vajiramandravi.com/current-affairs/india-ai-governance-guidelines-2025-towards-safe-inclusive-and-accountable-ai-ecosystem/

[22] Available at: https://ciso.economictimes.indiatimes.com/news/corporate/new-national-ai-regulation-in-india-what-can-tech-companies-expect/116884639

[23] Available at: https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en

[24] Available at: https://www.linkedin.com/pulse/indias-ai-inflection-point-20252030-productivity-capital-vpcnc

ISSN (O): 2584-2196

These evolving regulations and ethical standards are essential for India to maintain its competitive advantage in AI innovation. They also aim to create a digital society that values trust, fairness, and human rights. This adaptable governance framework can help position India as a global leader in responsible AI development, supporting economic growth while protecting individual privacy and community well-being.

CONCLUSION

As AI technologies develop quickly, regulatory frameworks need to change. India is likely to revise its Digital Personal Data Protection Act to include specific requirements for AI. These may involve mandatory audits, privacy impact assessments, and simpler processes for addressing grievances. This will improve protections for individuals in a changing technological environment.

India is at the crossroads where it can utilize its potential in artificial intelligence (AI) while simultaneously providing robust protection to privacy. The rapid rise of AI adoption, driven by a tech-savvy workforce and government initiatives, presents an opportunity for innovative development across health care, agriculture, and finance sectors. But this advancement has brought with it some pressing issues of privacy and the need for effective regulatory frameworks.

The proposed Personal Data Protection Bill and the Digital India Act are among the steps for building a convergent regulatory platform. However, existing laws with diverse structures often complicate how organizations comply. Furthermore, risk of data anonymization, how complex consent mechanisms may be built, and issues surrounding the proper balance between innovating and giving due respect to privacy rights may further help increase public trust and accountability.

These can be surmounted only by a focus from India on building an ethical framework in AI that makes its systems more transparent, accountable, and fair. Investing in privacy-preserving technologies, increasing public awareness of their rights with data, and creating public-private partnerships will form the bedrock for a sustainable AI ecosystem respectful of individual privacy.

ISSN (O): 2584-2196

As India continues to advance its AI capabilities, it will be crucial to strike the right balance between technological innovation and privacy protection. In doing so, India can position itself as a leader in ethical AI development while ensuring that the rights of individuals are protected in an increasingly digital world. This balanced approach will not only bolster India's AI governance but also contribute to a vibrant and responsible AI ecosystem that benefits all citizens.