Dr. Anand Kumar Dwivedi [Subject: Law] [I.F. 8.921] International Journal of Research in Humanities & Soc. Sciences

Vol. 14, Issue 08, August: 2026
ISSN(P) 2347-5404 ISSN(O)2320 771X

Artificial Intelligence and Data Privacy Laws in India

Dr. Anand Kumar Dwivedi
Assistant Professor, Department of Law
VSSD College, Kanpur
ORCID id - https://orcid.org/0009-0009-8256-1074

Abstract— The rapid adoption of artificial intelligence (AI) across India's public and private sectors has intensified debate over how the country's data privacy framework should respond to algorithmic decision-making, automated profiling, and large-scale personal data processing. This paper examines the evolving relationship between AI governance and data privacy law in India, tracing the legal foundations from the Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* through the Srikrishna Committee's 2018 report, the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), and the more recent Digital Personal Data Protection Rules, 2025. Drawing on statutory texts, government policy documents from NITI Aayog and the Ministry of Electronics and Information Technology (MeitY), and peer-reviewed and law-journal literature, the paper reviews India's regulatory approach to both data protection and artificial intelligence, and examines the points at which the two increasingly overlap, particularly through obligations placed on "Significant Data Fiduciaries" to assess algorithmic risk. The findings indicate that India has deliberately chosen not to enact a standalone AI law, instead relying on a lighter, voluntary governance framework layered onto its general data protection statute, with the result that data protection law is emerging as the country's de facto instrument for algorithmic accountability. The paper concludes that while this approach offers regulatory flexibility, it leaves significant gaps around explainability, automated decision-making, and algorithmic bias that will need to be addressed as AI adoption deepens across Indian institutions.

Keywords: artificial intelligence; data privacy; Digital Personal Data Protection Act; algorithmic accountability; India; right to privacy

INTRODUCTION

India's digital economy has expanded rapidly over the past decade, accompanied by a parallel expansion in the use of artificial intelligence across sectors ranging from financial services and healthcare to law enforcement and public administration. This growth has occurred against the backdrop of a data protection framework that, until recently, remained fragmented, resting largely on provisions of the Information Technology Act, 2000, and subordinate rules that predate the current scale of algorithmic data processing. The legal landscape began to shift decisively in August 2017, when a nine-judge bench of the Supreme Court of India held, in *Justice K.S. Puttaswamy v. Union of India*, that the right to privacy is a fundamental right protected under Articles 14, 19, and 21 of the Constitution, a ruling that directly shaped subsequent debate over what a comprehensive Indian data protection law should look like.

Following this judgment, the Ministry of Electronics and Information Technology constituted a Committee of Experts under Justice B.N. Srikrishna, which in July 2018 submitted its report, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, along with a draft Personal Data Protection Bill. After several years of legislative revision, India enacted the Digital Personal Data Protection Act in August 2023, and the corresponding Digital Personal Data Protection Rules were notified by MeitY in November 2025, with the Act's substantive provisions being phased in through May 2027. Running in parallel to this data protection track, NITI Aayog, the government's apex policy think tank, published its National Strategy for Artificial Intelligence in 2018 and its Responsible AI framework documents in 2021 and 2022, while MeitY released the India AI Governance Guidelines in November 2025, opting for a voluntary, principles-based approach to AI regulation rather than a dedicated AI statute comparable to the European Union's Artificial Intelligence Act.

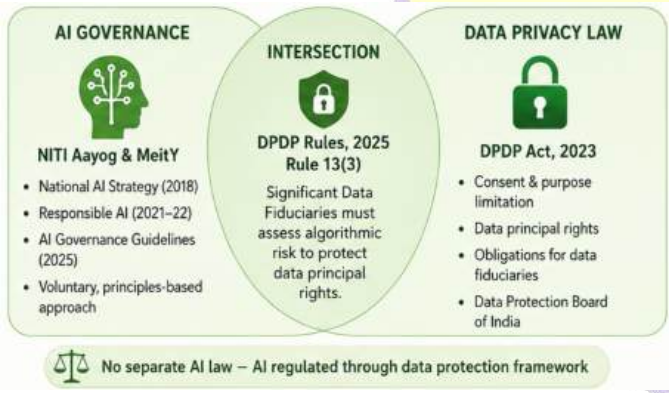
This paper examines how these two regulatory tracks, data privacy and AI governance, intersect in India's current legal landscape. It reviews the constitutional and statutory foundations of Indian data privacy law, surveys the country's AI policy framework, and analyses the specific points of convergence between the two, particularly the algorithmic risk-

Vol. 14, Issue 08, August: 2026
ISSN(P) 2347-5404 ISSN(O)2320 771X

assessment obligations recently introduced for large data processors under the DPDP Rules. In doing so, the paper aims to provide an integrated, evidence-based account of how India is, and is not, regulating the privacy implications of artificial intelligence.

Literature Review

The constitutional starting point for any discussion of Indian data privacy law is the Supreme Court's decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, decided on 24 August 2017. The nine-judge bench unanimously held that privacy is intrinsic to the right to life and personal liberty under Article 21 and is also protected under Articles 14 and 19, overruling earlier decisions in *M.P. Sharma v. Satish Chandra* and *Kharak Singh v. State of Uttar Pradesh* that had declined to recognise privacy as a standalone constitutional right. The judgment arose from a challenge to the constitutionality of the Aadhaar biometric identification scheme, and the Court, in recognising informational privacy as a component of the broader right, explicitly noted the need for a robust data protection framework capable of addressing the risks posed by large-scale data collection, profiling, and surveillance in the digital age. Legal commentary has since treated *Puttaswamy* as the foundational precedent underpinning virtually all subsequent Indian data protection legislation, and submissions made to the Srikrishna Committee itself drew directly on the judgment's reasoning.



Building on this constitutional foundation, the Committee of Experts chaired by Justice B.N. Srikrishna was constituted by MeitY in 2017 to examine India's data protection needs. Its December 2017 white paper and July 2018 final report, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, proposed a comprehensive regulatory framework built around the relationship between "data fiduciaries" and "data principals," borrowing conceptually from the fiduciary-duty model while adapting terminology to the Indian context. According to a summary published by the PRS Legislative Research policy analysis service, the Committee's report distinguished ordinary personal data from "sensitive personal data," such as data relating to caste, religion, and sexual orientation, and proposed that processing sensitive data require explicit consent, while also identifying four grounds on which data could be processed without consent, including where necessary for the state to perform welfare functions. The report and its accompanying draft bill went through several rounds of parliamentary revision before culminating, five years later, in the Digital Personal Data Protection Act, 2023.

The DPDP Act, enacted on 11 August 2023, establishes a comprehensive framework for the processing of digital personal data in India. According to its legislative text and subsequent legal commentary, the Act creates obligations for "data fiduciaries," defines the rights and duties of "data principals," establishes a Data Protection Board of India as the primary enforcement authority, and introduces a heightened compliance category, the "Significant Data Fiduciary," for entities whose scale or sensitivity of data processing poses greater risk. Analysis published by the law firm Morgan Lewis notes that once fully in force, the DPDP Act will replace the relevant provisions of the Information Technology Act, 2000, and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, which had previously served as India's primary, and widely criticised as inadequate, data protection framework. The Act's implementation has been phased: MeitY notified the Digital Personal Data Protection Rules, 2025, on 13 November 2025, bringing into force provisions relating to the establishment of the Data Protection Board, with the remaining substantive compliance obligations, including consent, notice, and security requirements, scheduled to take effect by May 2027.

Running alongside this data protection track, India's approach to artificial intelligence governance has developed through policy instruments rather than binding legislation. NITI Aayog's National Strategy for Artificial Intelligence, published in June 2018 under the banner "#AIforAll," identified healthcare, agriculture, education, smart cities and infrastructure, and smart mobility as priority sectors for AI deployment, and explicitly recommended establishing mechanisms to ensure AI is used responsibly, framing this as necessary to build public trust and enable large-scale adoption. NITI Aayog subsequently published a two-part Responsible AI approach document in 2021, dividing its ethical considerations into system-level and societal-level concerns, and followed this in 2022 with a use-case-specific discussion paper examining the risks of facial recognition technology, illustrating the government's preference for sector-specific, principles-based guidance over binding cross-sectoral regulation. This approach was reaffirmed in November 2025, when MeitY released the India AI Governance Guidelines, which, according to legal analysis published in the Indian Journal of Law and Legal Research, confirmed India's deliberate choice to rely on a "lighter, voluntary framework based on existing laws" rather

than adopt a comprehensive AI statute of the kind enacted by the European Union.

It is at this point that the data protection and AI governance tracks converge most directly. The same legal analysis notes that just nine days after releasing the voluntary AI Governance Guidelines, the government notified the Digital Personal Data Protection Rules, 2025, whose Rule 13(3) imposes a binding obligation on Significant Data Fiduciaries to conduct due diligence ensuring that any algorithmic software they deploy does not pose a likely risk to the rights of data principals. The article argues that this provision, although framed as an incidental data protection requirement, functions in practice as India's first binding algorithmic accountability mechanism, effectively regulating AI systems through the data protection framework rather than through dedicated AI legislation. A related body of legal commentary situates this development within a broader comparative debate: one comparative study of Indian and European Union AI governance models characterises the EU's approach as "rights-first, risk-based," with legally binding obligations and conformity assessments, in contrast to India's reliance on the DPDP Act, the National Strategy for Artificial Intelligence, and NITI Aayog guidance documents, which together constitute a more fragmented, principles-oriented regime.

Other recent legal scholarship has examined the adequacy of this approach. One analysis published on the intersection of AI and data protection in India argues that the DPDP Act's consent-based framework, together with data protection impact assessment requirements for Significant Data Fiduciaries, offers a plausible compliance pathway for AI systems but stops short of addressing algorithm-specific concerns such as explainability and bias, while also noting that parallel developments in evidentiary law, through provisions of the Bharatiya Sakshya Adhiniyam, 2023, are beginning to anticipate disputes over AI-generated outputs and audit trails. A separate research paper examining India's legal readiness for AI concludes that existing data protection law does not sufficiently regulate algorithmic accountability, automated decision-making, or consent-based processing specific to AI systems, and argues that the absence of AI-specific legal provisions increases the risk of privacy violations and discriminatory outcomes going undetected. Taken together, this literature suggests an emerging scholarly consensus that India's current framework treats AI governance largely as a subset of data protection compliance, an arrangement that offers some practical accountability mechanisms but leaves open significant gaps around algorithmic transparency and redress.

Objectives of the Study

This study is guided by the following objectives:

- To trace the constitutional and legislative evolution of data privacy law in India, from the recognition of privacy as a fundamental right to the enactment of the Digital Personal Data Protection Act.
- To examine India's policy approach to artificial intelligence governance, including the role of NITI Aayog and the Ministry of Electronics and Information Technology.
- To identify and analyse the specific points at which India's data protection and AI governance frameworks intersect.
- To assess the adequacy of the current framework in addressing algorithmic accountability, automated decision-making, and AI-specific privacy risks.
- To propose recommendations for strengthening the regulatory relationship between AI governance and data privacy law in India.

Research Methodology

This study employs a qualitative, doctrinal research design based on a review of primary legal sources and secondary academic and policy literature. Primary sources include the text of the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules, 2025, the Supreme Court's judgment in *Justice K.S. Puttaswamy v. Union of India*, and policy documents issued by NITI Aayog and MeitY, including the National Strategy for Artificial Intelligence, the Responsible AI approach documents, and the India AI Governance Guidelines. Secondary sources were identified through structured searches of Google Scholar, SSRN, and open-access law journal repositories, using combinations of the terms "artificial intelligence," "data protection," "India," "algorithmic accountability," and "Digital Personal Data Protection Act." Sources were included where they addressed India's data privacy or AI governance framework specifically, were drawn from a government body, court, or peer-reviewed or editorially reviewed law journal, and were verifiable through an accessible publication record, citation, or official

Vol. 14, Issue 08, August: 2026
ISSN(P) 2347-5404 ISSN(O)2320 771X

government repository. Sources that could not be independently verified were excluded from the review.

The review synthesises findings thematically, distinguishing between the data protection track and the AI governance track before examining their intersection, rather than conducting a new empirical or statistical analysis. As a literature- and document-based study, this paper does not involve primary data collection or fieldwork, and given the rapidly evolving and still partially unimplemented status of the DPDP Rules, 2025, at the time of writing, its conclusions should be read as reflecting the regulatory framework as currently enacted and phased in, rather than as a final assessment of a fully operative regime.

Legal and Regulatory Framework Governing Data Privacy in India

Constitutional Foundations: The Right to Privacy

India's data privacy framework rests on the constitutional recognition of privacy as a fundamental right established in *Puttaswamy*. The nine-judge bench held that privacy is protected under Articles 14, 19, and 21 of the Constitution, and explicitly overruled prior decisions that had denied privacy constitutional status. Beyond its immediate effect on the Aadhaar litigation from which it arose, the judgment articulated the need for the state to justify any infringement of privacy through a standard of proportionality, and recognised informational privacy, the ability of individuals to control data about themselves, as a distinct facet of the broader right. This constitutional foundation has since shaped the architecture of every subsequent Indian data protection instrument, providing the underlying rights-based justification for statutory consent requirements, purpose limitation, and individual data rights.

From the IT Act to the Digital Personal Data Protection Act

Prior to the DPDP Act, India's data protection regime rested primarily on the Information Technology Act, 2000, as amended in 2008, and the associated 2011 rules on reasonable security practices for sensitive personal data, a framework widely regarded by legal commentators as inadequate to the scale and complexity of contemporary data processing. The DPDP Act, 2023, was designed to replace these provisions with a comprehensive framework centred on the relationship between data fiduciaries, who determine the purpose and means of processing personal data, and data principals, the individuals to whom the data relates. The Act establishes obligations of purpose limitation and data minimisation for fiduciaries, grants data principals rights including access, correction, and erasure, and creates the Data Protection Board of India as an adjudicatory and enforcement body, with the Telecom Disputes Settlement and Appellate Tribunal designated as the appellate authority. Notably, the Act introduces the category of "Significant Data Fiduciary" for organisations whose processing activities involve a higher volume or sensitivity of personal data, subjecting them to enhanced obligations including data protection impact assessments and, as will be discussed below, algorithmic risk due diligence.

The Srikrishna Committee and Legislative Evolution

The path from constitutional recognition to statutory enactment ran through the Srikrishna Committee's 2018 report, which proposed the fiduciary-principal terminology and consent architecture that would eventually be carried, in modified form, into the DPDP Act. The Committee's report also grappled with the question of non-consensual processing, identifying specific grounds, such as compliance with legal obligations or the performance of state welfare functions, under which data could be processed without individual consent, a framework that anticipated later debate over how AI-driven public service delivery systems would be permitted to process citizen data. The extended legislative journey from the Committee's 2018 draft bill to the eventual 2023 Act, including an intermediate Personal Data Protection Bill, 2019, and its subsequent withdrawal and redrafting, reflects the difficulty of translating a rights-based constitutional principle into workable statutory obligations for a rapidly digitising economy.

Artificial Intelligence Governance in India

NITI Aayog's Responsible AI Framework

India's approach to AI governance has been shaped primarily by NITI Aayog, which was tasked by the government with establishing guidelines and policies for AI development and use. Its 2018 National Strategy for Artificial Intelligence set out priority sectors for AI deployment and explicitly identified ethics, privacy, and security as critical considerations for responsible AI adoption, while stopping short of proposing binding regulatory obligations. This was followed by the 2021 Responsible AI approach document, which organised its recommendations around system-level and societal-level considerations, and the 2022 discussion paper on facial recognition technology, which examined design-based and rights-based risks associated with a specific, publicly deployed AI use case, the Digi Yatra passenger processing system. Across these documents, NITI Aayog has consistently favoured a principles-based, sector-specific approach over comprehensive cross-sectoral legislation, reflecting a stated policy preference for balancing innovation with citizen protection rather than imposing prescriptive technical mandates.

The India AI Governance Guidelines and the Absence of AI-Specific Law

Vol. 14, Issue 08, August: 2026
ISSN(P) 2347-5404 ISSN(O)2320 771X

This policy orientation was most recently confirmed in the India AI Governance Guidelines, released by MeitY on 5 November 2025. According to legal analysis of the guidelines, they formalise India's decision not to enact a dedicated AI statute, opting instead for a framework grounded in existing laws, a choice explicitly contrasted with the European Union's comprehensive Artificial Intelligence Act. This decision reflects a broader pattern visible across NITI Aayog's prior publications: rather than creating a new regulatory body or licensing regime specifically for AI systems, the Indian government has chosen to embed AI-related obligations within existing legal instruments, most significantly, as discussed below, within the data protection framework itself.

The Intersection of AI and Data Privacy Law

Algorithmic Accountability under the DPDP Rules

The clearest point of convergence between India's AI governance and data protection tracks lies in Rule 13(3) of the Digital Personal Data Protection Rules, 2025, notified just days after the voluntary AI Governance Guidelines. This provision requires Significant Data Fiduciaries to exercise due diligence to ensure that algorithmic software they deploy in connection with data processing does not pose a likely risk to the rights of data principals. Legal analysis of this provision characterises it as functioning, in practice, as India's first binding algorithmic accountability mechanism, even though it is framed within the Rules as an incidental data protection due-diligence obligation rather than as a dedicated AI regulation. This arrangement means that, for the subset of large-scale data processors classified as Significant Data Fiduciaries, algorithmic risk assessment becomes a binding compliance obligation, while AI systems deployed by smaller entities, or those not directly tied to personal data processing, remain governed only by the voluntary guidance issued by NITI Aayog and MeitY.

Consent, Automated Decision-Making, and Data Principal Rights

The DPDP Act's consent-centred architecture also shapes how AI systems may lawfully process personal data in India. Data principals are entitled to give, manage, and withdraw consent, in some cases through a registered "consent manager," and fiduciaries are obligated to process data only for purposes to which the data principal has consented or which fall within the Act's specified exceptions. For AI systems that rely on large volumes of personal data for training or inference, this consent framework, together with the Act's purpose limitation and data minimisation principles, imposes real, if general, constraints on data collection and reuse. However, legal commentary notes that the Act does not expressly address automated decision-making or provide an explicit right to explanation comparable to provisions found in the European Union's General Data Protection Regulation, leaving individuals with comparatively limited statutory recourse when an algorithmic system, rather than a human decision-maker, produces an adverse outcome.

Gaps and Regulatory Challenges

Despite the emergence of Rule 13(3) as a de facto algorithmic accountability mechanism, legal scholars point to significant gaps in India's current framework. Analysis of the interaction between AI and data protection in India highlights that compliance pathways such as data protection impact assessments apply specifically to Significant Data Fiduciaries, leaving a large portion of the AI ecosystem, including smaller firms and public-sector deployments that may not meet the significance threshold, without an equivalent binding obligation. Other commentary argues more directly that existing data protection law does not sufficiently address algorithmic bias, transparency, or automated decision-making, and that the absence of AI-specific legislation increases the risk that privacy violations and discriminatory outcomes will go undetected or unremedied. These critiques suggest that while India's strategy of regulating AI indirectly through data protection law offers a pragmatic, flexible starting point, it may prove insufficient as algorithmic systems become more deeply embedded in decisions affecting credit, employment, insurance, and access to public services.

Discussion

The evidence reviewed in this paper indicates that India has deliberately chosen a layered, rather than unified, approach to regulating artificial intelligence and data privacy. Constitutional recognition of privacy as a fundamental right in *Puttaswamy* provided the normative foundation for a comprehensive data protection statute, which took shape through the Srikrishna Committee's 2018 report and culminated in the DPDP Act, 2023, and its 2025 Rules. Running in parallel, NITI Aayog and MeitY have consistently favoured voluntary, principles-based guidance for AI governance over binding, AI-specific legislation, a preference reaffirmed as recently as November 2025. The near-simultaneous release of the voluntary AI Governance Guidelines and the binding Rule 13(3) algorithmic due-diligence obligation illustrates how these two tracks have effectively merged in practice: rather than creating a standalone AI regulator, India is using its data protection statute as the primary lever for imposing binding obligations on AI systems, at least for the largest and most significant data processors.

This arrangement carries both advantages and risks. On one hand, embedding algorithmic accountability within the existing data protection framework avoids the delay and complexity of negotiating a wholly new regulatory regime, and leverages an enforcement body, the Data Protection Board of India, that is

already being established under the DPDP Act. On the other hand, the scope of binding algorithmic obligations under Rule 13(3) is currently limited to Significant Data Fiduciaries, leaving a substantial portion of AI deployment, particularly by smaller firms, research institutions, and certain public-sector applications, governed only by non-binding guidance. The literature also identifies a more specific gap around automated decision-making: unlike some comparable international frameworks, the DPDP Act does not establish an explicit individual right to an explanation of automated decisions, meaning that data principals affected by an algorithmic outcome may have limited statutory tools for contesting it directly. These gaps suggest that India's current framework, while a meaningful advance on its pre-2023 legal position, remains a work in progress rather than a settled resolution of the tension between AI innovation and individual privacy rights.

Recommendations

Based on the evidence reviewed, the following recommendations are proposed for policymakers, regulators, and researchers working on AI governance and data privacy in India.

The scope of binding algorithmic due-diligence obligations under the DPDP Rules should be reviewed periodically to determine whether the Significant Data Fiduciary threshold appropriately captures the range of AI systems that pose meaningful risk to data principals, including smaller-scale but high-impact deployments in sectors such as lending and recruitment.

The Data Protection Board of India should develop specific guidance clarifying how Rule 13(3)'s algorithmic risk due-diligence requirement applies in practice, including what constitutes adequate documentation and testing of algorithmic systems prior to deployment.

Policymakers should consider whether a more explicit right to explanation or contestability for automated decisions is needed within the data protection framework, given that the current Act does not clearly address this dimension of algorithmic accountability.

NITI Aayog and MeitY should continue to monitor whether the current voluntary, principles-based approach to AI governance remains adequate as adoption deepens, and should be prepared to introduce binding sector-specific rules, particularly for high-risk applications such as facial recognition and automated public service eligibility determinations, where voluntary guidance alone may prove insufficient.

Future legal research should track the practical implementation and enforcement of Rule 13(3) as it becomes operative, given that its function as a de facto AI governance instrument is, at the time of writing, a matter of legal interpretation and analysis rather than tested regulatory practice.

Conclusion

India's regulatory response to the intersection of artificial intelligence and data privacy has developed through two parallel, and only recently converging, tracks. Constitutional recognition of privacy as a fundamental right in *Puttaswamy* laid the groundwork for a comprehensive statutory data protection regime, realised through the Digital Personal Data Protection Act, 2023, and its 2025 Rules, while artificial intelligence governance has been shaped primarily through voluntary, principles-based guidance issued by NITI Aayog and MeitY, most recently through the India AI Governance Guidelines. The evidence reviewed in this paper shows that these two tracks are increasingly intertwined in practice, with the Digital Personal Data Protection Rules' algorithmic due-diligence obligation for Significant Data Fiduciaries functioning as India's first binding mechanism for algorithmic accountability, even though it was not designed as, and is not framed as, dedicated AI legislation. This pragmatic, layered approach offers real regulatory traction while leaving open significant gaps around automated decision-making, explainability, and the treatment of AI systems that fall outside the Significant Data Fiduciary threshold. As artificial intelligence becomes further embedded in decisions affecting Indian citizens' access to credit, employment, and public services, the adequacy of this data-protection-led approach to AI governance will remain an important and unsettled question for policymakers, courts, and researchers alike.

References

[1] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna. (2018). *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*. Ministry of Electronics and Information Technology, Government of India.
[2] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in
[3] Digital Personal Data Protection Rules, 2025. Ministry of Electronics and Information Technology, Government of India (notified 13 November 2025).
[4] Indian Journal of Law and Legal Research. (2026). Algorithmic accountability by the back door: The Significant Data Fiduciary due diligence mandate as India's de facto AI governance instrument. *Indian Journal of Law and Legal Research*. https://www.ijllr.com/post/algorithmic-accountability-by-the-back-door-the-significant-data-fiduciary-due-diligence-mandate-as
[5] *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, (2017) 10 SCC 1; AIR 2017 SC 4161 (Supreme Court of India).
[6] Ministry of Electronics and Information Technology. (2025). *India AI Governance Guidelines*. Government of India.

[7] NITI Aayog. (2018). *National Strategy for Artificial Intelligence #AIforAll*. Government of India. https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
[8] NITI Aayog. (2021). *Responsible AI for All: Approach Document for India, Part 1 – Principles for Responsible AI*. Government of India. https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf
[9] NITI Aayog. (2022). *Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology*. Government of India.
[10] PRS Legislative Research. (2018). Report summary: A Free and Fair Digital Economy. https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy
[11] *Why We Need Data Protection Laws for AI in India*. (2025). *De Facto Law Journal*. https://defactolawjournal.org/papers/why-we-need-data-protection-laws-for-ai-in-india/