



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Legal Aspects of Artificial Intelligence in India

~*Adhyan Rastogi*

ABSTRACT

Artificial intelligence is increasingly being used across sectors such as healthcare, finance, law enforcement, and public administration in India, yet the country still lacks a dedicated legal framework to regulate its development and use. This paper examines the existing legal and regulatory framework applicable to AI in India, with particular focus on the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and sector-specific guidelines issued by regulators such as the Reserve Bank of India and the Securities and Exchange Board of India. It also analyses key legal issues arising from the deployment of AI, including liability for AI-caused harm, intellectual property, algorithmic bias, deepfakes, automated decision-making, and AI-powered State surveillance. Further, the paper considers India's current policy initiatives, including the IndiaAI Mission, and compares India's approach with international developments, particularly the European Union's AI Act. It concludes that while India's existing legal framework provides a useful starting point, it is not sufficient to address the complex challenges posed by artificial intelligence. The paper argues that India should adopt a dedicated, risk-based legislative framework that promotes innovation while ensuring accountability, transparency, and the protection of fundamental rights.

I. Introduction

India has shown significant interest in the development of artificial intelligence, but its regulatory framework has not kept pace. On one hand, the Government approved the IndiaAI Mission in March 2024, committing ₹10,371.92 crores to make India a global hub for AI

development.¹ On the other hand, India still has no dedicated legislation governing AI development or deployment. There is no statute dealing with liability for autonomous systems, no framework requiring algorithmic transparency, and no regulator specifically responsible for overseeing AI-related risks across different sectors.

This gap between ambition and governance is not unique to India. Most countries are still working to regulate a technology that develops faster than the legislative process can keep pace with. However, the absence of a dedicated regulatory framework has greater consequences in the Indian context. AI systems are already being used in high-stakes areas such as judicial bail prediction, credit scoring, healthcare diagnostics, targeted advertising, and welfare benefit allocation. The risk of harm is also greater because of India's large population, the digital literacy gap, and limitations in the enforcement of existing laws.

This paper looks at the legal aspects of AI in India in four parts. First, it examines the existing statutory framework, mainly the Information Technology Act, 2000² and the Digital Personal Data Protection Act, 2023,³ and considers whether it is equipped to deal with the challenges created by AI. It argues that this framework was not designed for AI and cannot adequately regulate it. Second, it examines the sector-specific guidance issued by the Reserve Bank of India and the Securities and Exchange Board of India. Third, it discusses the legal issues arising from AI deployment, including liability, intellectual property, algorithmic bias, deepfakes, and state surveillance. Finally, it examines India's current policy approach and argues for a risk-tiered legislative framework based on the EU AI Act but adapted to India's own needs. The main argument of this paper is that India's existing legal framework is not sufficient to regulate AI.

The paper further argues that the Digital Personal Data Protection Act, 2023 provides an important foundation for AI regulation, but by itself it is not enough. It concludes that continued delays in introducing dedicated AI legislation could have constitutional, commercial, and geopolitical consequences for India.

II. The Global AI Regulatory Landscape: Context for India

¹ Cabinet Committee on Economic Affairs, Government of India, IndiaAI Mission: Approval of ₹10,371.92 Crore for Implementation (Mar. 7, 2024).

² Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

³ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDP Act].

To understand India's approach to AI regulation, it is important to consider the international developments in this area. In recent years, several countries have taken significant steps to regulate AI. Among them, the European Union's Artificial Intelligence Act, adopted in 2024, is the most comprehensive legislation on AI to date.⁴ It follows a risk-based approach by classifying AI systems into four categories: unacceptable risk, which is prohibited; high risk, which is subject to strict pre-market requirements; limited risk, which must comply with transparency obligations; and minimal risk, which is largely left unregulated. High-risk AI systems, including those used in critical infrastructure, employment decisions, credit scoring, migration, and the administration of justice, must meet requirements relating to data governance, technical documentation, transparency, human oversight, accuracy, and robustness before they can be placed on the EU market.

The United States has adopted a different approach by relying mainly on executive action instead of comprehensive legislation. In October 2023, it issued the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence⁵, which directed federal agencies to issue sector-specific guidance and introduced reporting requirements for developers of frontier AI models. However, it did not create binding legal obligations for the private sector. China, on the other hand, has introduced targeted regulations for specific AI applications. Its 2023 Interim Measures for the Management of Generative Artificial Intelligence Services require providers of generative AI services to comply with registration, content review, and watermarking requirements, reflecting China's focus on content control alongside AI safety.

Apart from these major jurisdictions, Singapore's Model AI Governance Framework and the OECD AI Principles provide a more principles-based approach that has been easier for many developing countries to adopt.⁶ India has referred to these frameworks in its own policy documents, but they have not been incorporated into binding law. During India's G20 Presidency in 2023, the New Delhi Leaders' Declaration endorsed international AI governance principles based on safety, trustworthiness, and inclusivity.⁷ While this demonstrated India's intention to contribute to the development of global AI standards, that

⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689 [hereinafter EU AI Act].

⁵ Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Nov. 1, 2023) (U.S.) (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence).

⁶ Info-Communications Media Development Authority, Singapore, Model AI Governance Framework (2d ed. 2020); OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (May 22, 2019).

⁷ G20 New Delhi Leaders' Declaration, ¶ 49 (Sept. 9–10, 2023) (endorsing international AI governance principles including safety, trustworthiness, and inclusivity).

role would be stronger if these principles were supported by domestic legislation rather than policy documents alone.

The differences between international approaches create both a challenge and an opportunity for India. The challenge is that Indian companies operating globally must already comply with the EU AI Act when using AI in European markets, which creates a practical compliance burden even though India does not yet have its own domestic AI law. The opportunity is that India can study the early difficulties faced by the EU model and design a framework better suited to its own institutions and development needs.

III. The Existing Indian Legal Framework Applicable to AI

India's existing legal framework was not designed to regulate AI. The Information Technology Act, 2000, which is the primary law governing cyberspace and digital transactions, recognises electronic records and digital signatures, and deals with cybercrime and intermediary liability. However, it does not contain any provisions specifically addressing autonomous systems, algorithmic decision-making, or the liability of AI developers and deployers.⁸ Section 43A of the IT Act, read with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,⁹ imposes a negligence-based duty of care on bodies corporate handling sensitive personal data. Although this provision can apply where AI systems process personal data, its scope is limited. It was not designed to address AI-generated inferences, and its enforcement has been limited in practice.

The Bharatiya Nyaya Sanhita, 2023,¹⁰ which replaced the Indian Penal Code, contains provisions on cheating, fraud, defamation, and obscene publication that can apply to AI-related harms. For example, a deepfake video created using generative AI could give rise to defamation liability, while an AI system used to carry out financial fraud could attract the cheating provisions. However, applying criminal law to AI raises difficult questions about the attribution of *mens rea* (criminal intent) to systems that do not possess human agency. Indian criminal law has not yet addressed how liability should be determined when harm is caused by an autonomous system rather than a natural person, and the existing legal framework provides no clear answer.

⁸ Information Technology Act, 2000, *supra* note 2.

⁹ Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

¹⁰ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India) [hereinafter BNS].

The Consumer Protection Act, 2019 provides another legal remedy that is relevant in the context of AI, although it has not received much attention in discussions on AI governance.¹¹ The Act imposes product liability on manufacturers and service providers for harm caused by defective products and deficient services. If an AI system used as a product or service causes harm to a consumer, such as a diagnostic AI tool incorrectly identifying a malignancy or a credit AI wrongly rejecting a loan application, the product liability provisions of the Consumer Protection Act may apply. The Central Consumer Protection Authority has the power to order the recall of defective products and impose penalties. However, it is still unclear whether these powers extend to AI systems, and the absence of technical standards for identifying AI-related defects makes enforcement difficult.

The Companies Act, 2013 raises an important question in the context of AI. If a company's board of directors delegates important business decisions, such as investment strategies, credit policies, or Human resource decisions, to an AI system, do the directors continue to remain responsible for the outcomes?¹² Section 166 of the Companies Act requires directors to exercise due care and skill and to act in the best interests of the company with reasonable diligence. Delegating important decisions to AI systems without adequate oversight raises questions about whether directors are fulfilling this statutory duty. Indian corporate law has not yet addressed the responsibilities of company boards in relation to the deployment of AI, even as AI systems are playing a greater role in corporate decision-making.

The Competition Act, 2002 is also relevant to AI, although this aspect has received limited attention in Indian legal scholarship.¹³ One concern is algorithmic pricing, where competing firms use AI-driven pricing algorithms that, even without any explicit coordination, arrive at similar pricing outcomes. This may raise concerns under Section 3 of the Competition Act, which prohibits anti-competitive agreements. Although the Competition Commission of India has not yet dealt with algorithmic collusion directly, the issue has already emerged in several other jurisdictions and is likely to arise before Indian tribunals in the future.

IV. The Digital Personal Data Protection Act, 2023 and Artificial Intelligence

¹¹ Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019, Ch. VI (India) (governing product liability for defective products and deficient services).

¹² Companies Act, 2013, No. 18, Acts of Parliament, 2013, § 166 (India) (imposing duties of care, skill, and loyalty on directors, including the duty to act in the best interests of the company).

¹³ Competition Act, 2002, No. 12, Acts of Parliament, 2002, § 3 (India) (prohibiting anti-competitive agreements).

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the most significant legislation relevant to AI in India today. This is not because it was enacted specifically to regulate AI, but because AI systems rely heavily on personal data, and the DPDP Act governs the processing of such data at every stage of the AI lifecycle.¹⁴ The Act imposes obligations on Data Fiduciaries, which are entities responsible for determining the purpose and means of processing personal data, and these obligations have important implications for AI development and deployment. Under Section 6, personal data can be processed only for the specific purpose for which free, specific, informed, unconditional, and unambiguous consent has been obtained. This creates a significant challenge for AI training. Machine learning models are often trained using datasets originally collected for purposes other than AI development, such as web-scraped data, historical transaction records, and user-generated content collected over time. However, the Act does not clearly state whether such existing data can lawfully be used for AI training without obtaining fresh, purpose-specific consent.

Section 7 of the DPDP Act identifies certain 'legitimate uses' under which personal data may be processed without consent, including processing necessary for the performance of a contract, compliance with the law, medical emergencies, and public interest functions of the State. However, it remains unclear whether AI model training falls within any of these categories. A narrow interpretation would limit legitimate uses to clearly defined operational purposes and exclude AI training, while a broader interpretation could allow AI training if it is reasonably connected to the services provided by the Data Fiduciary. The draft Digital Personal Data Protection Rules, published for public consultation in 2025,¹⁵ do not clarify this issue, leaving developers and deployers without clear regulatory guidance.

The principle of data minimisation, which requires personal data to be processed only to the extent necessary for the stated purpose, does not fit easily with the way AI systems are developed. Large language models and deep neural networks rely on diverse and extensive datasets to improve their performance, whereas the Act requires only the minimum amount of data necessary for a particular purpose to be processed. This creates a practical challenge in applying the principle of data minimisation to AI training.

Sections 12 and 13 of the DPDP Act give Data Principals the right to access, correct, and erase their personal data, as well as the right to seek grievance redressal. In the context of AI,

¹⁴ DPDP Act, *supra* note 3.

¹⁵ Ministry of Electronics and Information Technology, Draft Digital Personal Data Protection Rules, 2025 (Jan. 3, 2025) (India) (published for public consultation; does not contain explicit provisions on AI training or automated decision-making).

the right to erasure raises an important legal and technical question. If a Data Principal exercises the right to erase their personal data after it has been used to train an AI model, should the model itself be modified or retrained to remove the influence of that data? The Act does not address this issue. This is particularly significant because even under the GDPR, European regulators have not reached a clear legislative or regulatory position on how the 'right to be forgotten' should apply to trained AI models.

One of the most significant gaps in the DPDP Act is the absence of any provision dealing with automated decision-making. Article 22 of the GDPR gives individuals in the European Union the right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects, except in limited circumstances where safeguards such as human review and the right to challenge the decision are available. The DPDP Act does not contain a similar provision. As a result, in India, a person may be denied a loan, refused employment, charged a higher insurance premium, or even flagged as a criminal risk by a fully automated AI system without any legal right to seek human review, an explanation, or challenge the decision. This raises important constitutional concerns.¹⁶ In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised the right to privacy, including informational self-determination, as a fundamental right under Article 21 of the Constitution.¹⁷ Decisions made solely by AI systems without transparency or an effective remedy may be inconsistent with this constitutional guarantee. However, there is currently no statutory mechanism that allows affected individuals to enforce this right in the context of AI.

A comparison with the EU framework helps highlight this difference. In Europe, the GDPR and the EU AI Act work together. The GDPR regulates the processing of personal data throughout the AI lifecycle, while the EU AI Act imposes additional obligations on high-risk AI systems, including requirements relating to technical robustness, human oversight, and transparency. In contrast, India has the DPDP Act, which performs a role similar to the GDPR, but it has no equivalent legislation like the EU AI Act. As a result, India still lacks a dedicated legal framework to regulate high-risk AI systems.

V. Sector-Specific AI Regulation in India

¹⁶ DPDP Act, supra note 3, §§ 12–13 (conferring rights of access, correction, erasure, and grievance redressal on Data Principals).

¹⁷ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India) (nine-judge bench unanimously recognising privacy, including informational self-determination and the right against surveillance, as a fundamental right under Article 21 of the Constitution).

In the absence of comprehensive AI legislation, India's sectoral regulators have issued guidelines that provide the closest thing to AI regulation currently in force.

The Reserve Bank of India has taken the most structured approach. Its Digital Lending Guidelines, issued in 2022, require algorithmic credit underwriting models to be explainable to borrowers and prohibit regulated entities from relying entirely on automated systems for significant credit decisions without human review.¹⁸ This is the closest India currently comes to a safeguard similar to Article 22 of the GDPR. In addition, the RBI's framework on model risk management requires banks and non-banking financial companies to establish governance mechanisms for models used in credit, market risk, and liquidity management, including validation, continuous monitoring, and proper documentation.

The Securities and Exchange Board of India has regulated algorithmic trading since 2012 by requiring exchanges and brokers to implement safeguards such as pre-trade risk checks, real-time monitoring, and kill switch mechanisms for automated trading systems.¹⁹ Although SEBI's framework deals with AI in a limited context, it addresses an important area because high-frequency trading algorithms can influence markets within milliseconds, and the risks associated with unchecked algorithmic trading have been recognised in several market disruption events around the world.

The Insurance Regulatory and Development Authority of India has also issued guidelines allowing the use of AI in underwriting and claims processing, subject to requirements of fairness and non-discrimination.²⁰ These guidelines are intended to ensure that AI-driven underwriting does not result in discriminatory premium pricing based on inferred factors such as a person's location, social network, or behavioural patterns. They recognise that AI systems can reproduce and even amplify discriminatory outcomes, even where a protected characteristic is not directly used.

Within the judiciary, the Supreme Court of India introduced the SUPACE (Supreme Court Portal for Assistance in Courts Efficiency) AI tool to assist judges in processing case

¹⁸ Reserve Bank of India, Guidelines on Digital Lending, RBI/2022-23/111 DOR.CRE.REC.66/21.07.001/2022-23 (Sept. 2, 2022) (India) (requiring explainability of algorithmic credit decisions and mandating human oversight for significant credit determinations).

¹⁹ Securities and Exchange Board of India, Broad Guidelines on Algorithmic Trading, CIR/MRD/DP/09/2012 (Mar. 30, 2012) (India).

²⁰ Insurance Regulatory and Development Authority of India, Guidelines on the Use of Artificial Intelligence in Underwriting and Claims Processing, IRDAI/LIFE/MISC/CIR/2023 (2023) (India) (permitting AI use subject to fairness and non-discrimination requirements).

documents and identifying relevant precedents.²¹ SUPACE is intended to assist judges rather than replace judicial decision-making, with the final decision continuing to rest with the judge. However, its use raises important questions about transparency, algorithmic accountability in the judicial process, and the possibility of AI-assisted legal research introducing bias into case preparation. At present, there is no formal regulatory framework governing the use of AI in the judiciary in India.

The healthcare sector presents one of the most significant regulatory challenges for AI in India. Diagnostic AI systems capable of detecting malignancies, analysing radiological images, and predicting clinical deterioration are used in situations where errors can have serious and irreversible consequences. Although the Central Drugs Standard Control Organisation's guidance on Software as a Medical Device covers certain AI diagnostic tools, it remains limited in scope. In addition, the National Medical Commission has not yet introduced a comprehensive regulatory framework governing the use of AI in clinical settings.

VI. Key Legal Issues in AI Deployment

6.1 Liability for AI-Caused Harm

The question of who should be held liable when an AI system causes harm is one of the most important unresolved legal issues in India. Indian tort law, which has developed around the actions of human actors, does not apply easily to autonomous systems. Responsibility for a harmful outcome may lie with the developer who created the AI, the entity that trained it, the organisation that deployed it, or the user who applied it in a particular situation. However, the existing legal framework does not provide a clear basis for determining how liability should be allocated among them.

The doctrine of absolute liability, laid down by the Supreme Court in *M.C. Mehta v. Union of India*,²² provides one possible approach to determining liability for AI in high-risk situations. Under this doctrine, enterprises engaged in inherently dangerous activities are absolutely liable for any harm caused, regardless of fault. AI systems used in healthcare, autonomous vehicles, or critical infrastructure could be treated as inherently dangerous, making the

²¹ Supreme Court of India, SUPACE: Supreme Court Portal for Assistance in Courts Efficiency, <https://supace.sci.gov.in> (last visited June 2026) (AI research assistance tool launched by the Supreme Court of India for use by judges).

²² *M.C. Mehta v. Union of India*, (1987) 1 SCC 395 (India) (formulating the principle of absolute liability for enterprises engaged in inherently dangerous activities as distinct from the common law rule in *Rylands v. Fletcher*).

deployer strictly liable for any resulting harm. However, a more balanced approach would be to determine liability based on the level of risk posed by the AI system. Under such a framework, strict liability could apply to high-risk AI systems that cause personal injury or significant financial harm, while negligence-based liability could apply to lower-risk AI applications.

The Consumer Protection Act, 2019 provides another basis for addressing AI-related harm.²³ Under Chapter VI of the Act, product liability applies where a defective product or deficient service causes harm to a consumer. If an AI system is offered as a product or service, such as a health monitoring application, an automated insurance claims processor, or a credit-scoring tool, it could attract product liability if the harm results from a defect in its design, manufacturing, or inadequate instructions. However, enforcing these provisions remains difficult because there are no technical standards that clearly define what amounts to a 'defect' in an AI system. Even so, the existing framework provides a useful foundation for developing AI-specific product liability rules.

6.2 Intellectual Property in AI-Generated Works

The Copyright Act, 1957 recognises copyright in works created by authors, a concept that is based on human creativity. This raises important questions about the ownership of works generated by AI systems.²⁴ Indian law does not clearly address whether AI-generated works qualify for copyright protection, who should be regarded as the author of such works, or whether using copyrighted material to train AI models amounts to copyright infringement. Although the Delhi High Court has seen cases touching on AI-generated content, it has not yet given a definitive ruling on these issues. As a result, the legal position in India remains uncertain, particularly regarding the liability of developers who train AI models using copyrighted content without a licence, an issue that is also being considered by courts in the United States and Europe.

6.3 Algorithmic Bias and Discrimination

AI systems trained on historical data can reproduce and even amplify the biases already present in that data. In India, this is a serious concern because historical discrimination based

²³ Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019, Ch. VI (India) (governing product liability for defective products and deficient services).

²⁴ Copyright Act, 1957, No. 14, Acts of Parliament, 1957, § 2(d) (India) (defining 'author' in terms presupposing human creation, without addressing AI-generated works).

on caste, gender, religion, and region is often reflected in datasets used for credit, employment, healthcare, and law enforcement. Articles 14 and 15 of the Constitution prohibit discrimination on these grounds. However, it is still unclear how these constitutional protections apply to private entities that use AI systems, as Indian constitutional law has not yet fully resolved the horizontal application of fundamental rights. In addition, there is no specific legislation dealing with algorithmic discrimination in areas such as private employment, credit, or housing, leaving affected individuals without a clear legal remedy.

6.4 Deepfakes, Disinformation, and AI-Generated Harmful Content

Generative AI has made it much easier and cheaper to create convincing synthetic media, including deepfake videos, voice clones, and fabricated images. Such content can be used to defame individuals, spread electoral disinformation, or commit financial fraud. The Bharatiya Nyaya Sanhita (BNS) contains defamation provisions that can apply to this type of content, while the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021²⁵ require online platforms to remove flagged content. The misuse of AI during elections is a particularly serious concern. AI-generated audio and video of political candidates have already circulated during Indian state elections, raising concerns about the integrity of the electoral process. Although the Election Commission of India has issued advisories on the use of AI in political advertising, it does not have statutory authority to require the disclosure of AI-generated electoral content or to compel platforms to adopt detection mechanisms. As a result, these advisories are not legally binding, and India's current legal response has not kept pace with the growing challenge posed by deepfakes.

6.5 AI and State Surveillance: Constitutional Dimensions

The use of AI by State authorities raises constitutional concerns that are different from those arising in the private sector. One of the most significant issues is the use of AI-powered facial recognition systems by the Delhi Police and several other State police forces without any statutory authorisation or independent oversight.²⁶ India does not have a legal framework that regulates when facial recognition technology may be used, the accuracy standards it must satisfy, or the safeguards needed to prevent misidentification. As a result, individuals may be

²⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India), as amended by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023.

²⁶ Internet Freedom Foundation, *Watching the Watchers: A Report on Facial Recognition in India (2022)* (documenting deployment of facial recognition by Delhi Police, Telangana Police, and other state forces without statutory authorisation).

subjected to State surveillance or even wrongful detention based on AI systems whose error rates, training data, and algorithmic functioning are not publicly disclosed.

In the *Puttaswamy* judgment, the Supreme Court recognised privacy as a fundamental right under Article 21 and acknowledged that surveillance must satisfy the tests of legality, necessity, and proportionality.²⁷ At present, AI-based surveillance systems used by State authorities in India do not clearly satisfy these requirements. There is no specific law authorising their use, their proportionality has not been established, and their necessity has not been demonstrated through a transparent public process. This makes the use of AI for State surveillance one of the most significant constitutional issues in India, and it is a question that has not yet been directly considered by a higher court.

VII. The IndiaAI Mission and India's Policy Framework

The Government of India approved the IndiaAI Mission in March 2024 with a budget allocation of ₹10,371.92 crores over five years. The Mission is built around seven pillars: AI computing infrastructure, foundational model development, a datasets platform, application development, future skills, startup financing, and safe and trusted AI.²⁸ The 'Safe and Trusted AI' pillar focuses on developing indigenous AI safety tools, establishing an India AI Safety Institute, and strengthening India's participation in international AI safety initiatives, including the AI Safety Summits hosted by the United Kingdom and the Republic of Korea.

NITI Aayog published its National Strategy for Artificial Intelligence in 2018, setting out its 'AI for All' vision across five priority sectors.²⁹ It later published the Responsible AI for All report in 2021, which identified key principles for the ethical development of AI, including fairness, accountability, transparency, privacy, and security.³⁰ The Parliamentary Standing Committee on Communications and Information Technology submitted a report on AI in 2023, recommending the establishment of a dedicated AI regulatory framework and calling for amendments to the IT Act to address AI-specific liability.³¹ Although these policy documents provide useful guidance and draw from international best practices, they are

²⁷ Justice K.S. *Puttaswamy* (Retd.) v. Union of India, (2017) 10 SCC 1 (India) (nine-judge bench unanimously recognising privacy, including informational self-determination and the right against surveillance, as a fundamental right under Article 21 of the Constitution).

²⁸ Cabinet Committee on Economic Affairs, Government of India, IndiaAI Mission: Approval of ₹10,371.92 Crore for Implementation (Mar. 7, 2024).

²⁹ NITI Aayog, National Strategy for Artificial Intelligence: #AIForAll (June 2018).

³⁰ NITI Aayog, Responsible AI for All: Adopting the Framework — A Use Case Approach on Responsible AI (2021).

³¹ Standing Committee on Communications and Information Technology, Lok Sabha, Artificial Intelligence: Issues Relating to Ethics, Safety, and Accountability (Mar. 2023) (recommending dedicated AI regulatory framework and IT Act amendments for AI liability).

advisory in nature and do not have the force of law. As a result, there remains a gap between these policy recommendations and the absence of legislation to implement them.

VIII. Critical Analysis: The Cost of Principled Drift

India's current approach to AI governance can best be described as relying on non-binding policy documents, limited sector-specific guidance, and the absence of dedicated legislation. This creates risks in three important areas.

The constitutional risk is the most significant. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy, including informational self-determination, as a fundamental right under Article 21.³² However, India's current approach to AI does not adequately protect this right. The constitutional concerns are not merely theoretical. AI-powered facial recognition used by the Delhi Police has reportedly led to wrongful identifications, AI-linked Aadhaar systems have resulted in the exclusion of vulnerable individuals from welfare benefits without an effective remedy, and bail prediction tools used in some jurisdictions have assessed individuals without disclosing the criteria on which those assessments were based. In each of these situations, AI systems affect fundamental rights such as liberty, dignity, equality, and privacy without adequate transparency, accountability, or an effective mechanism to challenge their decisions. Although a writ petition is available in principle, it is not a practical remedy for most individuals affected by algorithmic harm.

The commercial implications are equally important. As Indian technology companies and startups develop AI products for global markets, the absence of a domestic AI regulatory framework creates legal uncertainty in areas such as product design, investor due diligence, and cross-border data flows. Companies developing AI for use in the European market must comply with the EU AI Act regardless of whether India has similar legislation. As a result, the absence of a comparable Indian framework does not reduce their regulatory burden; instead, it requires them to comply with foreign regulations without the support of equivalent domestic standards. This also means that Indian AI development is influenced largely by the EU's regulatory approach rather than by India's own legal framework, raising concerns about regulatory sovereignty in the field of AI.

³² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) (nine-judge bench unanimously recognising privacy, including informational self-determination and the right against surveillance, as a fundamental right under Article 21 of the Constitution).

The geopolitical and reputational implications should also be considered. India has established itself as a leader in digital governance through initiatives such as India Stack and the Digital Public Infrastructure model, both of which have received international recognition. However, the absence of a credible AI regulatory framework could weaken this position and allow other jurisdictions, such as the European Union and China, to play a greater role in shaping global AI standards. India's contributions to AI governance through the G20 would also carry greater weight if they were supported by domestic legislation.

It is often argued that regulating AI too early could slow innovation. While this concern has some merit, it is not entirely convincing. The EU AI Act follows a risk-based approach in which most AI applications, classified as limited or minimal risk, remain either unregulated or subject only to basic transparency requirements. India could adopt a similar approach without affecting AI applications used in areas such as customer service, productivity, content creation, and logistics. Regulatory obligations would apply only to AI systems that pose significant risks to fundamental rights or public safety. In comparison, the impact of such targeted regulation on innovation is limited when weighed against the constitutional, commercial, and reputational risks of continuing without a dedicated legal framework.

IX. Recommendations

First, India should enact dedicated legislation to regulate AI based on a risk-based framework. At a minimum, the legislation should identify prohibited uses of AI, such as social scoring by State authorities and indiscriminate biometric surveillance in public places without statutory authorisation. It should also impose pre-deployment requirements, including conformity assessments, technical documentation, and human oversight, for high-risk AI systems used in healthcare, credit decision-making, employment screening, and law enforcement. In addition, the law should provide individuals with a right to an explanation for automated decisions that produce significant legal or similar effects and establish a specialised AI regulatory authority with the technical expertise required to enforce these provisions.

Second, the rules framed under the DPDP Act should be expanded to address AI-specific issues. These should include clear guidance on consent requirements for AI training data, a right to an explanation for individuals affected by significant automated decisions, an obligation on Data Fiduciaries using high-risk AI systems to conduct algorithmic impact

assessments before deployment and at regular intervals, and standards for privacy-preserving AI training methods such as federated learning and differential privacy.

Third, India should enact a separate statutory framework governing the use of AI by State authorities for law enforcement and surveillance. Such a framework should specify the circumstances in which facial recognition and other AI-powered surveillance technologies may be used, the accuracy standards they must meet, the independent oversight mechanisms that should apply, and the remedies available to individuals who are wrongfully affected. This follows the constitutional principles laid down in *Justice K.S. Puttaswamy (Retd.) v. Union of India* and addresses one of the most significant gaps in India's current AI regulatory framework.

Fourth, India should establish an AI regulatory sandbox similar to those introduced by the RBI and SEBI in the fintech sector. This would allow developers to test high-risk AI applications in a controlled environment under appropriate regulatory supervision. Such a framework would help India develop AI regulations based on practical experience and evidence rather than relying solely on practical experience.

Fifth, India should strengthen the technical capacity of its regulatory institutions and actively participate in international AI governance initiatives through organisations such as the OECD, the Global Partnership on AI, and bilateral cooperation frameworks. This would help ensure that emerging global AI standards take into account India's priorities and the interests of the Global South. At the same time, stronger domestic regulation would enhance India's credibility and influence in shaping international AI governance.

X. Conclusion

Artificial intelligence has become an integral part of many sectors in India. It is already being used in areas ranging from credit scoring and financial services to surveillance and healthcare, with significant implications for individual rights and economic activity. However, the legal framework governing AI remains fragmented. It relies on laws that were enacted for other purposes, applies them to AI by analogy, and is supplemented by non-binding policy documents that do not have the force of law.

The Digital Personal Data Protection Act, 2023 is the most significant legislative development relating to AI governance in India in recent years. Its provisions on consent, data minimisation, and the rights of Data Principals place important safeguards on the use of

personal data by AI systems. However, it is a data protection law, not a comprehensive law governing AI. It does not address automated decision-making, AI-specific liability, the use of AI for State surveillance, or the regulation of high-risk AI systems. As a result, the DPDP Act alone is not sufficient to meet India's AI governance needs.

India already possesses many of the constitutional, institutional, and policy foundations required to develop an effective AI governance framework. The *Puttaswamy* judgment provides a constitutional basis through the recognition of privacy and informational self-determination, while Parliament, existing regulatory bodies, and the judiciary provide the necessary institutional framework. India has also demonstrated its commitment to AI governance through the IndiaAI Mission and its role in the G20. What is still needed is dedicated legislation to translate these principles into enforceable law. Delaying such legislation has real consequences for individuals whose rights are increasingly affected by AI systems operating without adequate accountability, transparency, or legal oversight. In a constitutional democracy committed to the rule of law, this is an issue that can no longer be ignored.