Page 1300 - 1317 **DOI:** *https://doij.org/10.10000/IJLMH.1111633*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/

Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

From Boardroom to Bureaucracy: Mapping the Regulatory Gap in India's Artificial Intelligence Governance across the Public and Private Sectors

NAKIHRING KHUMLO[1]

ABSTRACT

The deployment of artificial intelligence across India's institutional landscape has reached a critical threshold. Algorithmic systems now determine welfare eligibility, assist judicial decision-making, enable predictive policing, assess corporate creditworthiness, and inform boardlevel deliberations. Yet India's regulatory response remains fundamentally fragmented and non-binding. The MeitY India AI Governance Guidelines of November 2025, the RBI FREEAI Framework of August 2025, and the SEBI Consultation Paper of June 2025 represent meaningful policy advances but do not establish legally enforceable obligations in either the government or corporate domain. This article argues that India's regulatory gap is systemic rather than sectoral. The same challenges of algorithmic opacity, accountability deficit, and fragmented liability arise whether AI is deployed by a corporation making credit decisions or a government agency determining welfare eligibility. Critically, the most consequential AI governance failures currently occurring in India are in bureaucracies rather than boardrooms: documented cases of Aadhaar linked welfare exclusion , the unregulated deployment of facial recognition surveillance without statutory basis or proportionality review, and AIassisted judicial tools operating without transparency safeguards illustrate the urgency of a governance response that extends beyond the corporate sector. Through doctrinal and comparative analysis drawing on the European Union, China, and the United States, this article proposes a unified statutory framework for India addressing AI governance across both public and private institutional domains. The framework integrates AI specific accountability obligations for government and corporate deployers alike, a risk-based classification system calibrated to India's constitutional commitments, enforceable redress mechanisms, and a coordinated institutional architecture anchored in statute rather than policy.

Keywords: *artificial intelligence; algorithmic accountability; India AI governance; public sector AI; corporate governance; regulatory framework; Aadhaar; facial recognition.*

[1] Author is a Student at School of Law, CHRIST (Deemed to be University), Bangalore, Karnataka, India.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

I. INTRODUCTION

Artificial intelligence is transforming India's institutional landscape with a speed and breadth that its legal frameworks have not matched. In corporate boardrooms, machine learning systems inform strategic decisions, determine creditworthiness, evaluate employee performance, and drive market trading. In government bureaucracies, AI tools determine who receives welfare benefits, assist judges in identifying relevant precedents, enable law enforcement agencies to predict criminal activity, and conduct biometric surveillance of citizens in public spaces.[2] These deployments share a common architecture of risk. Whether deployed by a private corporation or a government agency, AI systems introduce algorithmic opacity that undermines accountability, distribute decision-making authority across sociotechnical networks that existing legal doctrine cannot easily reassemble into coherent chains of liability, and transfer effective decision-making power from human agents who bear legal responsibility to computational processes that do not.[3] The legal challenge is not unique to the corporate sector, nor is it unique to the public sector. It is a challenge for Indian governance as a whole. India's regulatory response has, until recently, treated these challenges as separate policy problems. The Ministry of Electronics and Information Technology's India AI Governance Guidelines, unveiled on 5 November 2025, represent the most comprehensive governance framework India has yet produced.[4] The Reserve Bank of India's Framework for Responsible and Ethical Enablement of Artificial Intelligence, published on 13 August 2025, addresses financial sector AI governance.[5] The Securities and Exchange Board of India's Consultation Paper of June 2025 targets AI in securities markets.[6] Together, these instruments signal a meaningful shift in regulatory awareness. But they are oriented primarily towards the private sector, they remain non-binding, and they do not address what is, arguably, India's most urgent AI governance problem: the unregulated deployment of AI by government agencies making decisions that

[2] NASSCOM, India AI Maturity Report 2024 (2024); see also Ministry of Electronics and Information Technology, Gov't of India, India AI Governance Guidelines pt. 1 (Nov. 5, 2025), https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf [hereinafter MeitY Guidelines].

[3] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information 3–8 (Harvard Univ. Press 2015); Andrew Selbst et al., Fairness and Abstraction in Sociotechnical Systems, in Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency 59 (2019).

[4] MeitY Guidelines, supra note 2; Press Info. Bureau, Gov't of India, MeitY Unveils India AI Governance Guidelines under IndiaAI Mission (Nov. 5, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2186639.

[5] Reserve Bank of India, Report of the Committee on Framework for Responsible and Ethical Enablement of Artificial Intelligence (FREEAI) (Aug. 13, 2025), https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/FREEAIR130820250A24FF2D4578453F824C72ED9F5D58

[6] Securities and Exchange Bd. of India, Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets (June 2025),https://www.sebi.gov.in/reportsandstatistics/reports/jun2025/consultationpaperonguidelinesforresponsibleusageofaimlinindiansecuritiesmarkets_94687.html [hereinafter SEBI AI Consultation Paper].

directly affect citizens' fundamental rights. This article examines India's AI governance challenge across both institutional domains. It argues that the regulatory gap India confronts is systemic rather than sectoral, rooted in the absence of any statutory framework establishing enforceable accountability obligations for algorithmic decision-making, whether by government or by corporations. Drawing on comparative analysis of the European Union, China, and the United States, it proposes a unified statutory framework that addresses AI governance across both domains within a single, coherent legal architecture. The article proceeds in seven further parts.

II. THE DUAL DEPLOYMENT PROBLEM: SHARED GOVERNANCE CHALLENGES ACROSS SECTORS

The governance challenges that AI deployment creates are not sectorspecific. They derive from the inherent characteristics of AI systems their opacity, their distributed architecture, and their capacity for autonomous decision making and these characteristics operate identically whether the deploying entity is a corporation or a government agency. Three challenges are of particular significance.

The first is epistemic opacity. Modern machine learning systems, particularly deep learning models, generate outputs through processes that may not be interpretable even by their designers.[7] This characteristic of the "black box" problem creates a structural mismatch between what legal accountability requires and what AI systems can provide. Legal accountability is premised on the ability to reconstruct decision-making processes and evaluate them against normative standards. Where an AI system determines a credit application, dismisses an employee, denies a welfare benefit, or recommends a judicial outcome, and that determination cannot be explained in terms a reviewing body can assess, the foundational conditions of legal accountability are absent.

The second challenge is structural diffusion. The design, training, deployment, and maintenance of AI systems involves multiple actors operating across distinct stages of a technological lifecycle: developers who build the model, data providers who supply training inputs, vendors who maintain the system, and institutional deployers who apply it in specific contexts.[8] When harm occurs whether a citizen is wrongly denied welfare or a shareholder is harmed by

[7] Finale DoshiVelez & Been Kim, Towards a Rigorous Science of Interpretable Machine Learning, arXiv:1702.08608 (2017); Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy 9–13 (Crown Publishers 2016).

[8] Selbst et al., supra note 3, at 60; Matthew Scherer, Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, 29 Harv. J.L. & Tech. 353, 367–72 (2016).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

undisclosed algorithmic trading the question of which actor bears legal responsibility is often unanswerable under existing doctrine. Negligence law requires identification of a duty of care attributable to a specific party; product liability frameworks are poorly suited to probabilistic, selfadjusting systems; and government tort liability doctrine is ill equipped to address automated administrative decisions.

The third challenge is constitutional exposure. AI deployment by government agencies implicates fundamental rights in ways that corporate deployment does not in quite the same direct sense. When a government agency uses an AI system to determine welfare eligibility, conduct surveillance, or profile individuals for law enforcement purposes, the constitutional principles of equality under Article 14, privacy under Article 21, and freedom from arbitrary state action are directly engaged.[9] India's courts have developed robust doctrine in each of these areas. What they have not yet addressed is how these doctrines apply to algorithmic state action to decisions made not by human bureaucrats exercising discretionary judgment but by computational systems operating through statistical inference.

III. INDIA'S CURRENT REGULATORY LANDSCAPE: A STRUCTURAL ANALYSIS

A. Corporate Sector Instruments

The MeitY India AI Governance Guidelines, developed by a high-level drafting committee chaired by Professor Balaraman Ravindran of IIT Madras and constituted in July 2025, represent the government's most substantive corporate AI governance engagement to date.[10] Organised around seven normative principles Trust as the Foundation; People First; Innovation over Restraint; Fairness and Equity; Accountability; Understandable by Design; and Safety, Resilience, and Sustainability the Guidelines propose a principle-based, techno-legal approach that deliberately declines to enact a standalone statute.[11] Three new institutional bodies are proposed: the AI Governance Group, chaired by the Principal Scientific Adviser; the Technology and Policy Expert Committee; and the AI Safety Institute. All three remain to be formally notified or given statutory form.[12]

The RBI FREEAI Report of August 2025 provides twentysix detailed recommendations for regulated financial institutions, including board-approved AI policies, strengthened audit mechanisms, AI inventory maintenance, incident reporting systems, and consumer-facing

[9] India Const. art. 14; India Const. art. 21; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India) [hereinafter Puttaswamy].
[10] MeitY Guidelines, supra note 2; Press Info. Bureau, supra note 4 (noting committee chaired by Prof. Balaraman Ravindran, IIT Madras, constituted July 2025).
[11] MeitY Guidelines, supra note 2, pt. 2 (Seven Sutras).
[12] Id. pt. 2 (Institutional Architecture: AIGG, TPEC, AISI).

explainability standards for AI-driven credit decisions.[13] The SEBI Consultation Paper of June 2025 proposes that listed entities deploying AI designate senior management to oversee these systems, maintain interpretability records, and periodically share audit findings with SEBI.[14] Together, these instruments represent a materially improved corporate AI governance orientation. Their critical limitation is that they are non-binding. The Companies Act, 2013 does not address AI-driven decision-making.[15] The Digital Personal Data Protection Act, 2023 addresses data processing and individual privacy but does not establish accountability standards for algorithmic corporate decisions.[16]

B. Public Sector Instruments

The public sector dimension of India's AI governance landscape is even less developed. NITI Aayog's National Strategy for Artificial Intelligence, published in 2018, positioned AI primarily as a developmental tool.[17] NITI Aayog's subsequent Responsible AI Principles of 2021 articulated normative commitments to safety, reliability, fairness, accountability, and transparency but did not establish binding obligations for government agencies.[18] The Digital India programme and the National eGovernance Plan have progressively embedded AI and automated decision systems in government service delivery without accompanying legal frameworks for accountability or redress.[19]

No statute currently establishes enforceable standards governing the use of AI by government agencies in administrative decision-making. The Right to Information Act, 2005 provides citizens access to information held by public authorities but does not address algorithmic decision-making.[20] General administrative law principles require reasoned decisions by government officers but have not been authoritatively interpreted to apply to algorithmic outputs. The DPDP Act, 2023, which governs data processing rights, does not establish a statutory right to explanation for automated government decisions affecting individuals.[21]

[13] RBI FREEAI Report, supra note 5, chs. 4–5 (Recommendations 1–26).
[14] SEBI AI Consultation Paper, supra note 6, §§ 4–5.
[15] The Companies Act, 2013, § 166, No. 18, Acts of Parliament, 2013 (India).
[16] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[17] NITI Aayog, Gov't of India, National Strategy for Artificial Intelligence: #AIForAll (June 2018), https://www.niti.gov.in/sites/default/files/202303/NationalStrategyforArtificialIntelligence.pdf.
[18] NITI Aayog, Gov't of India, Principles for Responsible AI (2021), https://www.niti.gov.in/sites/default/files/202102/ResponsibleAI22022021.pdf.
[19] Ministry of Electronics and Information Technology, Gov't of India, Digital India Programme (2015), https://www.digitalindia.gov.in.
[20] The Right to Information Act, 2005, No. 22, Acts of Parliament, 2005 (India).
[21] The Digital Personal Data Protection Act, 2023, supra note 16; see also Arghya Sengupta, AI Governance in India: Law, Policy and Political Economy, 9 Indian L. Rev. 328, 335 (2024).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

C. The Interface Problem

The most analytically significant gap in India's current framework is the absence of any governance architecture addressing the intersection of government and corporate AI deployment. Government agencies increasingly rely on corporate AI vendors for core administrative functions: the Aadhaar identity system depends on algorithms developed and maintained by private technology providers; welfare distribution systems built on Aadhaar integration rely on corporate data processing infrastructure; predictive policing tools are supplied by private vendors to state police forces; and SUPACE, the Supreme Court's AIassisted legal research tool, is built on commercial AI infrastructure.[22]

In these hybrid deployments, the accountability gap is doubled. The government agency deploying the system bears no clear legal obligation to ensure algorithmic accountability. The corporate vendor supplying the system operates under no specific regulatory framework governing AI services to government clients. When harm occurs a citizen wrongly excluded from welfare benefits, an individual wrongly identified as a criminal suspect there is no clear legal mechanism for attributing responsibility or obtaining redress.

IV. Public sector AI deployment in India: case studies in unregulated algorithmic power

A. Judicial AI: The SUPACE System

The Supreme Court of India introduced SUPACE the Supreme Court Portal for Assistance in Court Efficiency in April 2021 under then Chief Justice S.A. Bobde as an AIbased tool designed to assist judges in processing caserelated information and identifying relevant legal precedents.[23] SUPACE analyses case facts, extracts relevant information, and presents research summaries to judges, functioning as an algorithmic research assistant within the judicial decision-making process. As of 2024, the system operates within the Supreme Court focused primarily on assisting judges with complex, dataheavy cases and has been developed in collaboration with IIT Madras.[24]

The deployment of AI within the judicial system raises acute governance concerns that have

[22] See generally Software Freedom Law Ctr., India, Deployment of Facial Recognition Technology for State Surveillance and Monitoring (Nov. 2024), https://sflc.in; Internet Freedom Found., Facial Recognition in India: Part I (Sept. 2020), https://internetfreedom.in.

[23] Press Info. Bureau, Gov't of India, Use of Artificial Intelligence in Supreme Court (2024), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2148356; Vakasha Sachdev, AI at the Supreme Court: What Is SUPACE?, The Wire (Apr. 9, 2021), https://thewire.in.

[24] Frontiers in Political Science, Greening the Justice System: Assessing the Legality, Feasibility, and Potential of Artificial Intelligence in Advancing Environmental Sustainability within the Indian Judiciary (2025), https://www.frontiersin.org/journals/politicalscience/articles/10.3389/fpos.2025.1553705/full.

been acknowledged even by senior judges. The opacity of SUPACE's operations means that when the system draws attention to certain precedents, judges and litigating parties cannot know how those cases were prioritised or whether the algorithmic suggestions reflect inherent biases in India's case law corpus.[25] The principles of natural justice require that parties have an opportunity to respond to the material that influences a decision against them. Where that material is generated by an AI system whose outputs are not disclosed to the parties, these principles are potentially compromised. Scholars and practitioners have noted that AI trained on historical Indian case law may perpetuate discriminatory patterns based on caste, gender, or class that have historically characterised judicial outcomes.[26]

No statutory framework governs the deployment or use of SUPACE. No transparency requirements mandate disclosure to litigating parties that AI-generated summaries have been used in their case. No audit mechanism ensures that the system's outputs are free from bias. No redress mechanism enables parties to challenge decisions influenced by AIgenerated material. The deployment proceeds entirely on the basis of administrative decisions of the Supreme Court itself, without legislative mandate, independent oversight, or enforceable accountability, a situation that sits uncomfortably with India's strong constitutional tradition of the rule of law.

B. Welfare Distribution: AadhaarLinked Algorithmic Exclusion

The Aadhaar biometric identity system, administered under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, has been progressively linked to welfare benefit delivery across India.[27] The Public Distribution System, PMKISAN agricultural income support, the Mahatma Gandhi National Rural Employment Guarantee Scheme, and numerous other social protection programmes have been conditioned on Aadhaar authentication, with biometric verification required to access entitlements.[28]

The human consequences of this algorithmic welfare architecture are documented and severe. Independent researchers documented that Jharkhand's biometric authentication system had a failure-to-match rate of 49 percent, meaning that nearly half of Aadhaar holders in that state could not be matched to their digital biometric identifier and were thereby denied their welfare

[25] Global Voices Advox, When the Judge Meets the Algorithm: AI Tools Entering India's Courts (Dec. 2025), https://advox.globalvoices.org/2025/12/05 ("[W]hen SUPACE draws attention to certain precedents, judges and litigants cannot know how exactly those cases were prioritized.").
[26] Ctr. for Law & Pol'y Research, Artificial Intelligence and Judicial Bias (Aug. 2021), https://clpr.org.in/blo g/artificialintelligenceandthecourts ("[A]I would reinforce . . . biases . . . in the name of better efficiency.").
[27] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).
[28] The Mahatma Gandhi National Rural Employment Guarantee Act, 2005, No. 42, Acts of Parliament, 2005 (India); PMKISAN, Ministry of Agriculture & Farmers' Welfare, Gov't of India (2019), https://pmkisan.gov.in.

entitlements.[29] Investigative reports and academic studies by economists including Jean Drèze and Reetika Khera documented at least thirteen cases in Jharkhand alone where Aadhaarlinked exclusions directly caused starvation deaths by preventing access to Public Distribution System grain or pension entitlements due to authentication failures.[30] The most widely documented case is that of Santoshi Kumari, an eleven year old Dalit girl from Simdega district who died on 28 September 2017 after her family's ration card was cancelled because it was not linked to their Aadhaar number; her family had gone without adequate food for eight days before her death.[31]

No legal framework required the government to conduct an algorithmic impact assessment before deploying Aadhaarlinked welfare systems. No statutory right exists for citizens to receive an explanation of why an automated system denied their welfare claim. No independent body has oversight authority over the algorithmic architecture of these systems. The grievance mechanisms that exist under individual scheme regulations are not designed to address systematic algorithmic failure. The Supreme Court's proceedings in Writ Petition (Civil) No. 494 of 2012, while raising significant issues about Aadhaar's constitutionality, did not result in the establishment of a statutory accountability framework for the system's algorithmic operations.[32]

C. Law Enforcement: Facial Recognition and Predictive Policing

Multiple Indian state governments have deployed or piloted AIbased facial recognition and predictive policing systems without any legislative mandate or accountability framework. India currently has approximately 170 facial recognition technology systems, with the highest concentrations in Maharashtra, Delhi, and Telangana.[33] The Telangana Police's deployment of facial recognition for public surveillance has been extensively documented and criticised for operating without a clear legal basis or proportionality review.[34] The Internet Freedom

[29] Reetika Khera, Aadhaar Failures: A Tragedy of Errors, 54 Econ. & Pol. Wkly. 50 (Apr. 6, 2019) (noting 49% failure-to-match rate in Jharkhand and 37% in Rajasthan per government data); see also Emily Berman, A Failure to "Do No Harm": India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy, 2018 P.M.C. 5741784.

[30] Jean Drèze et al., Aadhaar and Food Security in Jharkhand: Pain Without Gain?, 52 Econ. & Pol. Wkly. 50 (2017); Siraj Dutta & Mithilesh Kumar, Another Aadhaar-Related Starvation Death in Jharkhand, CounterView (Jan. 2018), https://www.counterview.net.

[31] Supriya Sharma, Jharkhand Death: Girl Dies of Hunger Because Her Family Did Not Have an AadhaarLinked Ration Card, Scroll.in (Oct. 12, 2017), https://scroll.in/article/854225; Supriya Sharma, No Aadhaar, No Food Ration: 11 Stories that Show the Jharkhand Child Death Was Not an Aberration, Scroll.in (Oct. 20, 2017), https://scroll.in/article/854587.

[32] Writ Petition (Civil) No. 494 of 2012 (India) (Aadhaar constitutionality proceedings); see also Puttaswamy, supra note 9.

[33] Software Freedom Law Ctr., India, Analysis of the Facial Recognition TechnologyEnabled Surveillance Landscape in India (Nov. 2024), https://sflc.in ("India has 170 FRT systems, 20 of which are operational"); SS Rana & Co., Facial Recognition Technology: A Growing Challenge for Privacy (Apr. 2025), https://ssrana.in.

[34] HyperVerge, Facial Recognition Privacy in India (Nov. 2025), https://hyperverge.co/blog/facialrecogniti onprivacyindia ("The use of facial recognition for surveillance by the Telangana Police has led to an upsurge in

Foundation has sent legal notices to the National Crime Records Bureau and Delhi Police against the use of facial recognition without any statutory basis or procedural safeguards.[35] In Maharashtra, individual officers have developed and deployed predictive policing systems through internal administrative processes, without formal approval, legal framework, or independent evaluation prior to deployment.[36]

The constitutional implications are direct and significant. The Supreme Court's landmark ninejudge bench judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India recognised the right to privacy as a fundamental right under Article 21, establishing that state intrusions on privacy must satisfy a threefold test of legality, legitimate aim, and proportionality.[37] Facial recognition surveillance in public spaces conducted by AI systems capable of identifying and tracking individuals across locations constitutes an interference with privacy that requires a specific legal basis meeting this test. No such legal basis exists for the overwhelming majority of facial recognition deployments in India. The systems are operated entirely under executive and administrative decisions, without parliamentary authorisation, judicial oversight, or enforceable accountability.

The risk of algorithmic bias is particularly acute. Research by the National Institute of Standards and Technology documented significantly higher error rates for facial recognition systems when applied to darker skinned individuals, women, and older persons.[38] The EU AI Act treats social scoring systems and AI tools used for individual criminal risk assessment as posing unacceptable risks. India has no equivalent prohibition. In the comparative absence of regulatory intervention, systems with documented demographic error disparities are being deployed for law enforcement identification in contexts where errors have immediate and serious consequences for those wrongly identified.

D. Digital Public Infrastructure and Automated Administrative Decisions

Beyond welfare and law enforcement, AI and automated decision systems are embedded in India's broader digital public infrastructure. The DigiYatra programme uses facial recognition

public concern regarding consent and transparency.").

[35] Internet Freedom Found., Facial Recognition in India: Part I, supra note 22.

[36] Software Freedom Law Ctr., India, Artificial Intelligence and Surveillance in India: 2025 Roundup (Jan. 15, 2026), https://sflc.in/artificialintelligenceandsurveillanceinindia2025roundup ("Smart Prahari, an AIbased platform . . . deployed in Washim, Maharashtra. The model . . . the apparent absence of any formal approval process, legal framework, or independent evaluation prior to deployment.").

[37] Puttaswamy, supra note 9, ¶¶ 180–85 (Chandrachud J.) (establishing threefold test of legality, legitimate aim, and proportionality for privacy intrusions).

[38] Patrick Grother et al., Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NIST Interagency Rep. 8280 (Nat'l Inst. of Standards & Tech. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (documenting significantly higher error rates for darker skinned individuals, women, and older persons).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

to enable paperless air travel, processing passengers' biometric data to match them against booking records.[39] The NITI Aayog's own analysis noted that DigiYatra links Aadhaar identification and biometric data without a consent mechanism that is clearly compliant with the data protection principles India has itself articulated. The FASTag electronic toll collection system uses automated licence plate recognition to process toll transactions without human review, creating automated liability records with limited dispute resolution mechanisms.[40] The Unified Payments Interface ecosystem increasingly incorporates AI-driven fraud detection systems that can automatically suspend or block accounts based on algorithmic risk assessments, affecting citizens' access to financial services without any statutory framework for notice, review, or appeal.

In each of these cases the pattern is the same: AI deployment proceeds by administrative decision without legislative mandate, without algorithmic impact assessment, without transparency to affected individuals, and without accessible redress mechanisms. The government is deploying significant algorithmic power over citizens' lives without the legal authorisation and accountability framework that the rule of law requires.

V. CORPORATE SECTOR AI GOVERNANCE: THE ACCOUNTABILITY DEFICIT

A. Fiduciary Duties Under the Companies Act, 2013

The Companies Act, 2013 provides the foundational framework for corporate governance in India. Section 166 establishes directors' fiduciary duties, requiring them to act in good faith in the best interests of the company and in the interests of shareholders and other stakeholders.[41] These duties are framed in general terms that presuppose human agency that directors exercise informed judgment based on accessible information, that their decisions can be evaluated against legal standards, and that responsibility for corporate outcomes can be attributed to identifiable individuals.

AI-driven corporate decision-making disrupts each of these presuppositions. The Act contains no provision requiring directors to ensure that AI systems used in corporate decision-making are auditable, explainable, or free from discriminatory bias. It establishes no standard of care applicable to reliance on algorithmic outputs. It imposes no disclosure obligation in relation to

[39] NITI Aayog, Gov't of India, Responsible AI for All: Adopting the Framework A UseCase Approach on Facial Recognition Technology (June 2024), https://www.niti.gov.in; Ministry of Civil Aviation, Gov't of India, DigiYatra Policy (July 2023), https://www.civilaviation.gov.in/sites/default/files/202307/Digi%20Yatra%20Policy%20(DIGI%20YATRA).pdf

[40] National Highways Authority of India, FASTag Programme Overview (2019), https://www.nhai.gov.in; Software Freedom Law Ctr., supra note 36.

[41] The Companies Act, 2013, § 166, supra note 15; Umakanth Varottil, The Evolution of Corporate Law in PostColonial India, 31 Am. U. Int'l L. Rev. 253, 271–75 (2016).

AI deployment in governance critical functions.[42] The consequence is that corporations may deploy AI systems in contexts with significant consequences for employees, customers, and shareholders determining hiring and firing, allocating credit, informing merger decisions without any mandatory audit, disclosure, or liability mechanism. The absence of enforceable obligations creates not merely a governance gap but a market failure: corporations that invest in robust AI governance bear costs that noncompliant competitors avoid.

B. Financial Sector Instruments and Their Limitations

The RBI FREEAI Report of August 2025 represents the most specific and actionable AI governance instrument in India's current regulatory landscape for the financial sector. Its twentysix recommendations include requirements for board approved AI policies, AI inventory maintenance, strengthened internal and third-party audit mechanisms, consumer-facing explainability standards for AI-driven credit decisions, incident reporting systems, and an AI innovation sandbox.[43] The SEBI Consultation Paper of June 2025 proposes that market participants deploying AI and machine learning designate senior management with technical expertise to oversee these systems, maintain validation, documentation, and interpretability records, and share audit findings with SEBI periodically. It also addresses cybersecurity risks associated with generative AI in capital markets, including the use of AI to produce fraudulent financial documents and deepfake content.[44]

Both instruments represent a meaningful step forward. Both, however, remain at the consultative or recommendation stage. Neither has been translated into binding regulatory requirements through RBI circular, SEBI regulation, or statutory amendment. The conversion of these recommendations into binding instruments through master circulars, listing obligation amendments, and prudential guidelines is the necessary immediate step that has not yet been taken.

C. The Liability Fragmentation Problem

AI-driven corporate decision-making introduces structural unaccountability that existing Indian liability doctrine cannot adequately address. Where an AI system makes a credit decision that discriminates against a protected class, or where an algorithmic trading system causes market disruption, the question of which party bears legal responsibility is often unanswerable under

[42] Maria Lillà Montagnani & Maria Lucia Passador, Fiduciary Duties and Business Judgment Rule 2.0 in the AI Act Age (June 9, 2025), https://ssrn.com/abstract=5714102 (arguing EU AI Act necessitates new AI-specific fiduciary duties); Companies Act, 2013, § 166, supra note 15.
[43] RBI FREEAI Report, supra note 5, chs. 4–5 (Recommendations 1–26, including Recommendation 2: BoardApproved AI Policy).
[44] SEBI AI Consultation Paper, supra note 6, §§ 4–5.

existing frameworks.[45] Developers design the model; data providers supply training inputs; vendors maintain the system; and corporations deploy it in specific contexts. Negligence law requires identification of a duty of care attributable to a specific actor. Vicarious liability presumes a hierarchical employment relationship. Both frameworks are poorly suited to the networked, multiparty structure of AI deployment. The MeitY Guidelines signal an intention to clarify AI liability through targeted amendments to the Information Technology Act, 2000, including clarification of the liability of AI developers, deployers, and users.[46] This commitment has not yet resulted in enacted law.

VI. COMPARATIVE FRAMEWORK: LESSONS FROM THE EU, CHINA, AND THE UNITED STATES

A. The European Union: Binding Obligations Across Both Sectors

The European Union's Artificial Intelligence Act, Regulation (EU) 2024/1689, which entered into force on 1 August 2024, is the world's most comprehensive enacted AI governance framework.[47] Its significance for India's dual governance challenge lies in the fact that it applies to both public and private deployers of AI. Government agencies and corporations face identical obligations where they deploy systems classified as high risk. High risk systems under Annex III include AI deployed in education, employment, creditworthiness assessment, essential services, law enforcement, migration, and the administration of justice.[48] Compliance obligations for deployers encompassing risk management, data governance, transparency enabling human oversight, technical documentation, and automatic logging apply whether the deployer is a private corporation or a public authority.

The Act's prohibition framework is particularly relevant for India's public sector deployments. Article 5 prohibits realtime biometric identification in publicly accessible spaces for law enforcement purposes, subject to narrow exceptions requiring prior judicial authorisation.[49] This prohibition directly addresses the unregulated facial recognition deployments documented in Section IV.C. The prohibition provisions became applicable on 2 February 2025. Full high

[45] Scherer, supra note 8, at 367–72; see also Luciano Floridi et al., An Ethical Framework for a Good AI Society, 28 Minds & Machines 689, 703 (2018).
[46] MeitY Guidelines, supra note 2, pt. 3 (Legal Gap Analysis, proposing targeted amendments to Information Technology Act, 2000 to clarify liability allocation between AI developers, deployers, and users).
[47] Commission Regulation 2024/1689, Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 2024/1689) (EU) [hereinafter EU AI Act].
[48] EU AI Act, supra note 47, Annex III (listing high risk categories including employment, creditworthiness, essential services, law enforcement, justice).
[49] Id. art. 5(1)(d) (prohibiting realtime remote biometric identification in publicly accessible spaces for law enforcement, with enumerated exceptions).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

risk system compliance obligations apply from 2 August 2026, with an extended transition for systems embedded in regulated products until 2 August 2027.[50] The key structural lesson for India is that treating algorithmic accountability as a governance obligation rather than a sectoral compliance requirement means the source of the obligation is the nature and risk level of the AI deployment, not the institutional identity of the deployer.

B. China: SectorSpecific Enforcement with Unified Principles

China's AI governance architecture offers India a different structural lesson: that sectorspecific enforcement, administered through existing regulatory relationships, can achieve meaningful accountability without a single comprehensive statute. China's layered approach, the Algorithm Recommendation Provisions of March 2022, the Generative AI Interim Measures of August 2023, and the AI Labelling Rules effective September 2025 establishes binding obligations through administrative instruments issued by the Cyberspace Administration of China.[51] By October 2025, Chinese authorities had approved thousands of algorithm filings under the mandatory registration system, demonstrating operational enforcement capacity.[52] The Cyberspace Administration's 2024 enforcement campaign targeting algorithmic abuses on major platforms resulted in corrective orders and investigations against platform operators, demonstrating that registration-based accountability translates into practice.[53]

China's framework applies to government-adjacent deployments as well as purely commercial ones. Systems with public opinion attributes or social mobilisation potential, a category that encompasses government information systems and public interest AI applications must undergo security assessments and CAC registration. China is simultaneously preparing a standalone Artificial Intelligence Law; the Standing Committee of the National People's Congress included AI legislation in its preliminary review agenda for 2024 and 2025, with a draft released for consultation in December 2025.[54] The lesson for India is that sectorspecific layering, using existing regulatory relationships and enforcement mechanisms, produces

[50] Id. art. 113; European Commission, The AI Act: Shaping Europe's Digital Future (2025), https://digitalstrategy.ec.europa.eu/en/policies/regulatoryframeworkai (noting prohibitions applicable from Feb. 2, 2025; high risk full enforcement from Aug. 2, 2026).

[51] Cyberspace Admin. of China, Administrative Provisions on Recommendation Algorithms in InternetBased Information Services (effective Mar. 1, 2022); Cyberspace Admin. of China, Interim Measures for the Administration of Generative AI Services (effective Aug. 15, 2023); Cyberspace Admin. of China et al., Measures for the Labelling of AIGenerated Content (effective Sept. 1, 2025).

[52] Int'l Ass'n of Privacy Profs., Global AI Governance Law and Policy: China (Oct. 2025), https://iapp.org/resources/article/globalaigovernancechina ("As of October 2025, China has approved thousands of algorithm filings.").

[53] Cyberspace Admin. of China, Qing Lang Governance of Typical Algorithmic Issues on Online Platforms (Nov. 12, 2024).

[54] CMS Expert Guide, AI Laws and Regulations in China (Feb. 2026), https://cms.law/en/int/expertguides/airegulationscanner/china.

functional accountability across both government and corporate domains without requiring a single comprehensive statute.

C. The United States: Executive Volatility as Cautionary Lesson

The United States provides India's most important cautionary lesson. The Biden Administration's Executive Order 14110 of October 2023, on Safe, Secure, and Trustworthy AI, directed federal agencies to develop safety standards, address algorithmic discrimination, and protect workers and consumers from AI-related harms.[55] This order was revoked by the Trump Administration's Executive Order 14148 on 20 January 2025, with the replacement Executive Order 14179 of 23 January 2025 characterising the Biden approach as having paralysed the AI industry.[56] The December 2025 Executive Order directing the Department of Justice to challenge state AI laws and establish a minimally burdensome national framework further illustrates that a governance philosophy centred on innovation promotion at the expense of accountability creates structural conditions in which citizens' rights are subordinated to industrial policy.[57]

India's 2025 policy instruments the MeitY Guidelines, the RBI FREEAI recommendations, and the SEBI consultation paper are precisely analogous to the prereversal Biden framework in their non-binding character. The US experience demonstrates directly where nonstatutory governance leads: accountability commitments that cannot survive a change in regulatory philosophy. For India, which aspires to governance continuity across administrations, statutory anchoring is not merely preferable but necessary.

VII. TOWARDS A UNIFIED REGULATORY FRAMEWORK FOR INDIA

A. RiskBased Classification Across Both Sectors

Drawing on the EU model, India should adopt a risk-based classification of AI systems calibrated to its constitutional commitments and institutional context. Three tiers are proposed, each applying to government and corporate deployers alike.

The first tier prohibited applications should include: AI systems that use biometric data to

[55] Exec. Order No. 14,110, Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75191 (Nov. 1, 2023).

[56] Exec. Order No. 14,148, Initial Rescissions of Harmful Executive Orders and Actions, 90 Fed. Reg. 8237 (Jan. 28, 2025) (revoking Exec. Order No. 14,110); Exec. Order No. 14,179, Removing Barriers to American Leadership in Artificial Intelligence, 90 Fed. Reg. 8741 (Jan. 31, 2025).

[57] Exec. Order, Ensuring a National Policy Framework for Artificial Intelligence (Dec. 11, 2025), https://www.whitehouse.gov/presidentialactions/2025/12/eliminatingstatelawobstructionofnationalartificialintelligencepolicy (directing DOJ AI Litigation Task Force to challenge state AI laws; conditioning broadband funding on state compliance with federal AI policy).

identify individuals in public spaces without specific statutory authorisation and prior judicial oversight; AI systems that assign social scores to citizens based on behavioural patterns; and AI systems in welfare administration that make final eligibility determinations without human review and an accessible appeals mechanism. These prohibitions should be enacted through amendment to the IT Act, 2000 or through new standalone AI accountability legislation.

The second tier high risk applications requiring mandatory compliance obligations should include AI systems used in: judicial and quasi-judicial decision-making; welfare eligibility determination; employment decisions; creditworthiness and financial product access; law enforcement prediction and profiling; and corporate decisions that materially affect the rights of shareholders, employees, or consumers. Compliance obligations for this tier should include predeployment algorithmic impact assessment, periodic third-party audit, human oversight and override capability, disclosure to affected individuals of the fact and nature of AI involvement in any decision affecting them, and incident reporting to the relevant regulatory authority.

The third tier standard risk applications should require registration with a mandatory AI disclosure register and basic transparency documentation, without the full compliance obligations of the high risk tier. Adapting China's algorithm registration model, this register should be administered by the proposed AI Governance Group and should be publicly accessible.

B. Statutory Accountability Obligations for Government Deployers

The most critical and currently absent element of India's AI governance framework is a set of enforceable accountability obligations for government agencies as AI deployers. The constitutional foundation for these obligations is already established. Article 14's prohibition of arbitrariness in state action applies to algorithmic state action.[58] Article 21's protection of life and personal liberty interpreted in Puttaswamy to encompass a right to privacy constrains biometric surveillance by the state.[59] The right to fair hearing, recognised as an element of constitutional due process since Maneka Gandhi v. Union of India, applies to administrative decisions regardless of whether they are made by human officers or algorithmic systems.[60] Statutory reform in this area does not require new constitutional doctrine; it requires the

[58] E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3, ¶ 85 (India) (establishing that Article 14 prohibits arbitrariness in state action, going beyond mere classification).
[59] Puttaswamy, supra note 9, ¶ 248 (Chandrachud J.) (recognising right to privacy as fundamental right under Article 21); id. ¶ 180 (establishing threefold test of legality, legitimate aim, and proportionality for state privacy intrusions).
[60] Maneka Gandhi v. Union of India, (1978) 1 SCC 248, ¶ 56 (India) (Bhagwati J.) (holding that procedure affecting fundamental rights must be fair, just, and reasonable; establishing constitutional due process in administrative decision-making).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

translation of existing constitutional principles into legislative form.

Four specific statutory reforms are required. First, an amendment to the Right to Information Act, 2005, or a standalone statutory provision, should establish that citizens have a statutory right to receive a meaningful explanation of any automated government decision that adversely affects their rights or entitlements. Second, government agencies deploying AI in high-risk categories should be required by statute to conduct algorithmic impact assessments before deployment, with public disclosure of the results. Third, the jurisdiction of existing administrative tribunals should be extended to receive and adjudicate complaints about algorithmic administrative decisions. Fourth, a statutory prohibition should be enacted on deploying AI systems in high risk government applications without prior parliamentary authorisation or subordinate legislation laid before Parliament.

C. Statutory Accountability Obligations for Corporate Deployers

For the corporate sector, four statutory reforms complement and reinforce the MeitY and RBI recommendations. First, Section 166 of the Companies Act, 2013 should be amended to incorporate a duty of algorithmic diligence an obligation on directors of companies deploying AI in material corporate decisions to maintain a board-approved AI governance policy, ensure periodic audit of high-risk AI systems, establish human override mechanisms, and disclose AI governance arrangements in annual reports.[61] This standard does not require directors to possess technical expertise equivalent to data scientists; it requires the engaged oversight that the duty of care has always demanded for complex specialised corporate functions.

Second, the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 should be amended to require listed companies deploying AI in governance critical functions to disclose the categories of AI deployment, the governance mechanisms in place, the results of any algorithmic audit, and the redress mechanisms available to affected parties.[62] Third, the RBI should issue a mandatory circular converting the FREEAI Report's recommendations into binding prudential requirements for regulated financial institutions. Fourth, a statutory presumption of civil liability for harms caused by AI systems that cannot be explained or attributed to identifiable human choices rebuttable upon demonstration of governance compliance should be enacted through amendment of the IT Act, 2000. This structure creates the correct incentive: it makes robust AI governance commercially rational, not merely

[61] Companies Act, 2013, § 166, supra note 15; Montagnani & Passador, supra note 42 (articulating concept of "AI due care" and "AI loyalty oversight" as dimensions of enhanced fiduciary standard under AI Act framework); cf. RBI FREEAI Report, supra note 5, Recommendation 2.

[62] SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (India); SEBI AI Consultation Paper, supra note 6, § 4.2.

aspirational.[63]

D. Redress Mechanisms and Statutory Institutional Architecture

Effective AI governance requires accessible redress mechanisms for individuals harmed by algorithmic decisions, whether made by government or corporate deployers. A statutory right to seek explanation, review, and appeal must apply in both sectors. The institutional architecture proposed in the MeitY Guidelines, the AI Governance Group, the Technology and Policy Expert Committee, and the AI Safety Institute provides a sound foundation that must be given statutory form.[64] The cautionary lesson of the US experience is that executive-accredited bodies are institutionally fragile. The AIGG should be constituted with statutory authority to receive complaints, conduct investigations, issue guidance binding on both government agencies and corporations, and refer matters to appropriate sectoral regulators. India's existing sectoral regulators MCA, SEBI, the RBI, the CCI, and TRAI must each be given explicit AI mandates through targeted legislative amendment enabling them to issue binding sectorlevel AI governance rules, conduct investigations, and impose penalties for noncompliance.

VIII. Conclusion

India stands at a decisive juncture in its engagement with AI governance. The policy architecture of 2025 the MeitY Guidelines, the RBI FREEAI Framework, and the SEBI Consultation Paper represents the most serious and specific engagement with AI governance India has yet produced. The Seven Sutras provide a normative foundation of genuine quality. The proposed AIGG, TPEC, and AISI offer an institutional architecture that, if given statutory form, would provide the coordination capacity that governance across two institutional domains requires.

This article has argued that the most significant limitation of India's current approach is its failure to address both institutional domains, government and corporate within a unified accountability framework. The most consequential AI governance failures currently occurring in India are in bureaucracies, not boardrooms. In Jharkhand's welfare system, algorithmic authentication errors contributed to documented starvation deaths among India's most vulnerable citizens. In public spaces across Maharashtra, Telangana, and Delhi, facial recognition surveillance systems operate without statutory basis, proportionality review, or

[63] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); MeitY Guidelines, supra note 2, pt. 3; cf. Council Directive 2024/2853 on Liability for Defective Products, 2024 O.J. (L 2024/2853) (EU) (providing EU model for liability safe harbour conditioned on compliance).

[64] MeitY Guidelines, supra note 2, pt. 2 (Institutional Architecture); Press Info. Bureau, Gov't of India, India AI Impact Summit 2026 (Feb. 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2228315.

oversight. In the Supreme Court itself, an AI research tool assists judicial decision-making without transparency to litigating parties or safeguards against bias. An AI governance framework that addresses only the corporate sector however carefully designed leaves these constitutionally sensitive deployments entirely unregulated.

The comparative models examined in this article together support a single central argument: effective AI governance requires statutory expression, applies uniformly across government and corporate deployers, and creates enforceable obligations rather than aspirational principles. The EU demonstrates that a risk-based framework can address both sectors simultaneously within a single binding instrument. China demonstrates that sectorspecific enforcement architecture, using existing regulatory relationships, can produce functional accountability across both domains. The US demonstrates, powerfully and cautionary, that a governance architecture premised on executive discretion and voluntary guidelines collapses when political conditions change.

India has the constitutional foundation, the institutional capacity, and now the policy intelligence to build a unified statutory AI governance framework. The constitutional commitments to fairness, equality, and dignity that animate Article 14 and Article 21 apply equally to the algorithm that determines whether a Dalit grandmother in Jharkhand receives her food ration and to the algorithm that determines whether a Mumbai professional receives a bank loan. The distance between boardroom and bureaucracy, in India's AI governance landscape, is not measured in institutional space. It is measured in the gap between the legal accountability that both domains require and the statutory framework that neither has yet received. Closing that gap is the defining AI governance imperative of this decade.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]