



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

AUTOMATION TO ACCOUNTABILITY: CORPORATE ARTIFICIAL INTELLIGENCE AND LEGAL GOVERNANCE IN INDIA

AUTHORED BY - HIMALYA CHAUHAN

Student, Master of Laws (LL.M.),

Faculty of Law, ICFAI University, Baddi, Himachal Pradesh, India.

CO-AUTHOR - DR. KESHVA NAND

Assistant Professor and Head of Department,

Faculty of Law, ICFAI University, Baddi, Himachal Pradesh, India.

Abstract

Corporate governance in India is undergoing a transformation due to algorithmic decision-support systems and corporate artificial intelligence is yet to receive comprehensive legislative attention. This paper tackles the problem of rapid integration, lagging governance. Using a doctrinal approach, supplemented by primary and secondary sources such as statutes and regulations, consultation papers, judicial rulings, and a selected body of scholarly works, the study explores Indian law on artificial intelligence as applicable to boards, corporate compliance, market activities, and data-centric comportment. India possesses a fragmented governance approach, embedded in the Companies Act, 2013, the SEBI framework, the Digital Personal Data Protection Act, 2023, and laws on cybersecurity and competition. However, these frameworks treat challenges of explainability, attribution, vendor lock-in, and the intersection of privacy and competition inconsistently. The study also illustrates that Indian Courts, along with the sectoral regulatory bodies, are gravitating towards proactive accountability as part of the governance of artificial intelligence, as opposed to a defence in the face of the use of AI technology in data-centric market activities. The main argument of the paper is that the governance of corporate artificial intelligence systems in India will not be successfully resolved with a single piece of comprehensive legislation. Rather, it needs a focus on the corporate governance design of accountable boards and sectoral convergence of the regulators of corporate law, securities, cyber, data protection, and competition law.

Keywords: Artificial Intelligence; Corporate Governance; Digital Personal Data Protection Act, 2023; Securities Regulation; Competition Law

Introduction

AI has quickly become a core practice in nearly all aspects of business management. This includes risk assessment, internal auditing, fraud detection, engagement with investors, forecasting in supply chains, the management of human resources, and even in some cases aiding board decision-making. Interestingly, in the field of corporate governance, AI has the potential to create, classify, and prioritize a corporation's information, and to determine the course of action the corporation should take. The real challenge for corporate governance is when AI begins to shape the mechanisms of oversight, compliance, and corporate disclosure. These challenges, like control, accountability, and the limits of the law concerning corporate governance, cannot be resolved through the improvement of technology alone.¹

What is unique in India's case is that AI adoption in the corporate world is happening at a much faster pace than the development of laws to regulate its corporate use. For the time being, corporate governance in India is primarily the result of an amalgamation of different laws and regulations such as the law on corporate governance, law on insider trading and securities regulation, law on data protection, and law on cybersecurity. The primary research question of the paper is whether this kind of law in its most fragmented and dispersed state has the potential to regulate the challenges and problems posed by AI when it becomes an integral part of the management and operational control systems of corporations in India. The main issue is not how technology is changing, but how the regulatory framework is structured.²

This Article posits that while the pieces of a governance framework are scattered across Indian law, they are still under-integrated and inconsistent. The main focus of this Article is corporate governance and Indian law, particularly with regard to listed companies, data-intensive business models, and market-bound applications of artificial intelligence. The author employs doctrinal legal research that combines analysis of statutory obligations, regulatory frameworks, and case law with select legal scholarship. The author argues that AI is a governance element that requires Board of Directors accountability, oversight that is subject to audit, and regulatory

¹ Organisation for Economic Co-operation and Development, "Artificial Intelligence in Society" 52 (2019).

² NITI Aayog, "National Strategy for Artificial Intelligence #AIForAll" 11 (June, 2018).

controls. Therefore, AI must not be regarded as a tool for efficiency and left to the discretion of managers.³

Artificial Intelligence as a Corporate Governance Problem

Artificial Intelligence (AI) is not only a component of corporate governance; it is also an organisational method for generating, classifying, and implementing information. The law must adapt to this new reality of systems where the outputs are often uncertain, opaque, and dependent on external service providers. Therefore, the law must include the concepts of stewardship, supervision, and accountability.⁴

Artificial Intelligence as Governance Infrastructure

Traditional company law defines governance as a system for balancing power, information, and oversight. Thus, corporate governance encompasses more than the composition of boards. It also refers to the systems and processes that regulate and constrain the actions of corporate managers. Contemporary scholarship views governance as a construct of incentives, controls, and accountability mechanisms, rather than a system of formal subsystems.⁵ In the context of the prioritization of risks, the detection of anomalies, and the recommendation of choices, the interface of artificial intelligence as a component of this system does indeed govern. It controls the information that is presented to the board, what issues are determined to be worthy of management's attention, and what issues are effectively rendered invisible to the corporate system.

The Indian perspective on governance is not dissimilar, with the board being responsible for establishing ethics, accountability, and managing the risks of the organisation. As AI is integrated and scaled, the potential of corporate governance systems is expanded, while the mechanisms of corporate governance remain opaque.⁶ Corporate boards are still responsible for the governance of the firm, even if complex algorithms are employed for compliance. As such tools become embedded in the management systems of a firm, governance tools, and systems are integrated into the management systems of a firm.

³ Reinier Kraakman, John Armour, et.al., *The Anatomy of Corporate Law: A Comparative and Functional Approach* 45 (Oxford University Press, Oxford, 3rd edn., 2017).

⁴ Woodrow Barfield and Ugo Pagallo, *Research Handbook on the Law of Artificial Intelligence* 84 (Edward Elgar Publishing, Cheltenham, 2nd edn., 2025).

⁵ Bob Tricker, *Corporate Governance: Principles, Policies, and Practices* 96 (Oxford University Press, Oxford, 5th edn., 2025).

⁶ Asish K. Bhattacharyya, *Corporate Governance in India: Change and Continuity* 146 (Oxford University Press, New Delhi, 1st edn., 2016).

Director Responsibility and Human Oversight

This point is supported by modern corporate governance theories which caution that automation should not be thought of as a substitution for human judgment at the highest levels of the organisation. Michael Hilb's idea of “artificial governance” is also helpful, for it views automation not merely as a tool of assistance, but a disruptive force to the extent that it can alter the very nature of boardroom discussions. In the case of Indian law, the focus must still be on human control.⁷ Artificial intelligence can help board members deal with complexity, but there is no substitute for the expectation that fiduciary duties and the duty of care are executed by real persons who will be held accountable.

Therefore, Section 166 of the Companies Act, 2013 is the most important law for analysing the Indian context of management board decisions to use artificial intelligence. This segment of the law is expressed in terms of the directors of a company having to (a) act in the good faith and for the benefit of the company, (b) discharge their duties with care, (c) diligence and (d) independent judgment. These requirements are almost impossible to meet in a governance framework where directors accept the outputs of governance algorithms without question, or where evaluative responsibility is simply contracted out to the vendors of the software.⁸ The use of artificial intelligence in corporate governance frameworks can be justified only if there is a human review and a rationale for its use and if the outputs of the software are questioned prior to their enactment.

Transparency, Auditability, and Contestability

The next question on governance is about transparency. In legal contexts, transparency is often understood as requiring the full disclosure of source codes. This is too limited a standard for corporate governance. The more relevant question is the extent to which a board can understand the objectives, purposeful training assumptions, risks of errors, and constraints on the operation of the system it approves. An example in this respect is Kieron O'Hara's analysis of explainable artificial intelligence.⁹ O'Hara argues that explanation is a social and institutional activity rather than simply a technological issue of software coding. For firms, this means that a significant explanation of a system or process must take into account the requirements for auditing, compliance, investor protection, and evidence collection.

⁷ Michael Hilb, “Toward Artificial Governance? The Role of Artificial Intelligence in Shaping the Future of Corporate Governance”, 24 *Journal of Management and Governance* 851 (2020).

⁸ The Companies Act, 2013 (Act 18 of 2013), s. 166.

⁹ Kieron O'Hara, “Explainable AI and the Philosophy and Practice of Explanation”, 39 *Computer Law & Security Review* 105474 (2020).

The same can be said about the scholarship on algorithmic regulation. This scholarship argues that governance of automated systems must include elements of design review, output monitoring, and the ability to identify and mitigate bias that is built into the system.¹⁰ Within a corporation, these elements may be audit committees, internal control systems, model validation and data governance systems, and contractual terms with third party suppliers. These elements include contestability provisions that may allow employees, consumers, counterparties, or compliance personnel to contest automated recommendations that are deemed to be erroneous or unfair. It is a symptom of a technical and governance failure, which would be the subject of a regulatory oversight, if a firm is unable to provide a reconstruction of the reasoning of an artificial intelligence system in flagging a transaction, arbitrarily denying a request, or assigning a risk an arbitrary position.

The Indian Legislative and Regulatory Architecture

There is no standalone corporate artificial intelligence code in Indian law. An artificial intelligence code is constructively found in Companies Act, Data Protection Act, IT Act, Securities and Exchange Board of India Act, Competition Act, and Public policy. The arrangement is extensive and offers functional coverage but, brings in standards, enforcement gaps, and uncertainty in coordination among institutions.¹¹

Company Law as the First Layer of Control

The first legal layer, Companies Act (2013), indirectly and materially governs AI through its provisions on the duties, structure and discipline of directors and of disclosure and financial controls. The absence of the term 'AI' in the Companies Act will not render it irrelevant to AI. The Companies Act, by its very form, is technology-neutral and that neutrality allows it to manage and regulate new organisational technologies via its existing standards. The Act's provisions on audit committees, internal audits, and financial controls mean that any substantial AI implementation that impacts reporting, compliance, or risk is adequately covered by the existing frameworks of oversight and supervision.¹²

The Act is especially important because it pushes against the common but incorrect assumption that technological complexity creates a zone of managerial insulation. Directors continue to be

¹⁰ Karen Yeung and Martin Lodge, *Algorithmic Regulation* 72 (Oxford University Press, Oxford, 1st edn., 2019).

¹¹ NITI Aayog, "Responsible AI: Approach Document for India, Part 1: Principles for Responsible AI" 18 (February, 2021).

¹² The Companies Act, 2013 (Act 18 of 2013), ss. 134(5)(e), 138, 177.

liable for the governance implications of systems that are chosen, bought, or provided on behalf of the company. This perspective is backed by the comparative corporate law literature, which highlights that corporate law assigns decision-making privileges and monitoring duties in order to contain agency expenses and informational gaps in a company. While artificial intelligence can potentially lower some information expenses, it can also complicate asymmetry if only the internal IT teams or outside contractors comprehend how a model undergoes training, updating, or is subjected to constraints.¹³

Data Protection, Significant Data Fiduciaries, and Board Accountability

Layer two pertains to the Digital Personal Data Protection Act of 2023, which becomes crucial in instances when corporate AI involves employee, customer, investor, or user data in digital form. The statute defines automated processing, applies to digital personal data processed within and in some instances outside India, and establishes the Data Protection Board of India as the adjudicating authority under the Act. As the statute is not restricted to AI, its requirements correlate directly with the risks of profiling, model training, and behavioural data inference and corporate data surveillance and targeting.¹⁴

Section 10 stands out more than others since it allows the Central Government to designate Significant Data Fiduciaries and mandates these organisations to appoint a locally based Data Protection Officer, along with an independent data auditor. This Section mandates the implementation of a Data Protection Impact Assessment and related audits at regular intervals.¹⁵ In more corporate governance terms, this sets out a clear link between data compliance and board accountability. A large organisation using AI in any of the aforementioned areas may soon face a governance model whereby board-level oversight of data practices will be structurally and mandatorily required.

The Act's value is in the balance of consent, reasonable security safeguards, breach notification, and marked distinctions on obligations and responsibilities. Relevant literature on AI has repeatedly illustrated that privacy-related harm does not end at breaches of the traditional sense. Privacy-related harm extends to discrimination, manipulation, and domination of one party over the other in the relationship concerning personal data.¹⁶ In that sense, the significance of

¹³ Reinier Kraakman, John Armour, et.al., *The Anatomy of Corporate Law: A Comparative and Functional Approach* 31 (Oxford University Press, Oxford, 3rd edn., 2017).

¹⁴ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), ss. 2(b), 3, 18.

¹⁵ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 10.

¹⁶ Rowena Rodrigues, "Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities", 4 *Journal of Responsible Technology* 100005 (2020).

the Act is beyond border compliance. It mandates a strict form of data governance that will impact design, contracts, retention policies, access, and response protocols for organisations that rely on AI.

Cybersecurity, Logging, and Incident Response

A third layer is created by the Information Technology Act, 2000, and the instructions of the Indian Computer Emergency Response Team, dated April 28, 2022. These instructions require the reporting of certain cyber incidents within six hours, state the need for designated points of contact, and apply compliance obligations to service providers, intermediaries, data centres, body corporates, and public agencies. Regarding artificial intelligence governance, operational resilience is the priority.¹⁷ Certain models such as trading, consumer-facing and fraud detection, and internal compliance are susceptible to data poisoning, credential stuffing, adversarial attacks, and unauthorized access to the model, all of which have significant governance implications.

The cyber layer is also significant because artificial intelligence usually enters the organisation through outsourced APIs, cloud-based services, and vendor tools. The legal governance of artificial intelligence is more and more about the governance failings related to the interfaces between the procurement processes and accountability, where contractual relationships mask the true picture. Therefore, Indian corporate governance must prioritize cybersecurity, access logging, and incident escalation as a crucial layer of artificial intelligence governance and not as a separate IT function.¹⁸ A board that implements automated systems without ensuring cyber resilience is, in effect, transferring governance risk until a cyber incident occurs, resulting in a lawsuit.

Securities Regulation and Listed Entity Governance

For listed entities and market intermediaries, the most sector-specific corporate governance tools offered by the Securities and Exchange Board of India are at present applicable. The cataloguing by the regulator began with the Reporting Circular for Market Intermediaries in

¹⁷ Indian Computer Emergency Response Team, “Directions under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe and Trusted Internet” (April, 2022).

¹⁸ Woodrow Barfield and Ugo Pagallo, *Research Handbook on the Law of Artificial Intelligence* 178 (Edward Elgar Publishing, Cheltenham, 2nd edn., 2025).

January 2019¹⁹, followed by similar circulars for Market Infrastructure Institutions²⁰ and Mutual Funds²¹. These tools obliged the reporting of Artificial Intelligence and Machine Learning tools that were being, or are, deployed in the Securities Market. While the tools had no punitive intent, their objective was to furnish information. They represented the first instance of the regulator formally acknowledging the fact that automated systems were being, and are, deployed to govern the markets and engage with investors.

This understanding developed further in the consultation paper released on 20 June 2025 concerning the responsible use of artificial intelligence and machine learning in Indian securities markets. The paper advanced a number of high-level principles concerning model governance and disclosure, testing and monitoring, fairness and bias, and data security. Although a consultation document, its doctrinal scope is somewhat broader, as it shifts the abstract governance constructs into the operational space of regulated entities.²² Artificial intelligence, therefore, is contextualized as an area of greater scale and an even more harmful potential, which justifies a greater degree of supervision, as opposed to some other innovations that require a degree of compliance.

The listed entity framework provided by the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, as amended, continues to be applicable. These regulations do not have AI-specific requirements. However, they do impose extensive requirements on the board's governance, risk management, control frameworks, related party transactions, material events, and the internal control environment.²³ For example, if listed companies use AI to impact revenue recognition, market disclosures, and communication with shareholders or to perform trading surveillance, these uses will need to be examined in light of the company's existing obligations. The question, therefore, is not whether AI is part of regulation, but whether the obligations are interpreted with the required level of technological intensity.

The cyber aspect of securities regulation also needs to be analysed separately. The

¹⁹ Securities and Exchange Board of India, "Reporting for Artificial Intelligence (AI) and Machine Learning (ML) Applications and Systems Offered and Used by Market Intermediaries" (Circular No. SEBI/HO/MIRSD/DOS2/CIR/P/2019/10, January 4, 2019).

²⁰ Securities and Exchange Board of India, "Reporting for Artificial Intelligence (AI) and Machine Learning (ML) Applications and Systems Offered and Used by Market Infrastructure Institutions" (Circular No. SEBI/HO/MRD/DOP1/CIR/P/2019/24, January 31, 2019).

²¹ Securities and Exchange Board of India, "Reporting for Artificial Intelligence (AI) and Machine Learning (ML) Applications and Systems Offered and Used by Mutual Funds" (Circular No. SEBI/HO/IMD/DF5/CIR/P/2019/63, May 9, 2019).

²² Securities and Exchange Board of India, "Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets" (June, 2025).

²³ The Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, regs. 4, 17, 30.

Cybersecurity and Cyber Resilience Framework issued by SEBI in August 2024 added a layered structure for cyber governance for all regulated entities. Where AI models are embedded within market systems, custody, advisory, or client interfaces, cyber resilience and governance integrity become indistinguishable.²⁴ A compromised model could provide distorted investment advice, inhibit the provision of alerts, or enable unauthorized access, without a traditional governance breach occurring. The legal perspective has to consider the integrity and resilience of the cyber systems that govern AI as part of fiduciary and regulatory obligations and not operational risk.

Competition Law and Public Policy

AI governance cannot be fully contained. The internal firm governance structure will be unable to contain the growing asymmetries in the competition across industries because of the advantages in data collection and model building. For this reason, the market study on AI and competition by the Competition Commission of India is a noteworthy policy contribution. The study recognizes competition distortions in AI markets, as well as issues of access to compute, datasets, and ecosystems.²⁵ This, on the whole, integrates the concepts of intra-firm governance with the governance of market structures. The AI governance strategy of a firm can impact the firm. It can legally enable the firm to extend its exclusionary power and to engage in digitally anti-competitive practices.

Public policy showcases the imbalance in India between the promotion of AI and its control. The Union Cabinet's approval of the IndiaAI Mission in March 2024 brought India a state policy that creates a fully integrated, end-to-end AI ecosystem. Figure 1 shows the allocation of resources to the various components of the AI ecosystem (as presented to Parliament).²⁶ The Indian government's strategy champions the development of both AI compute and AI innovation. Interestingly, the government allocates a far smaller proportion of the budget to the development of what the government terms 'safe and trusted AI.'

²⁴ Securities and Exchange Board of India, "Cybersecurity and Cyber Resilience Framework for SEBI Regulated Entities" (Circular No. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113, August 20, 2024).

²⁵ Competition Commission of India, "Market Study on Artificial Intelligence and Competition" (October, 2025).

²⁶ Cabinet Approves Ambitious IndiaAI Mission to Strengthen the AI Innovation Ecosystem, *available at*: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2012355> (last visited on May 21, 2026).

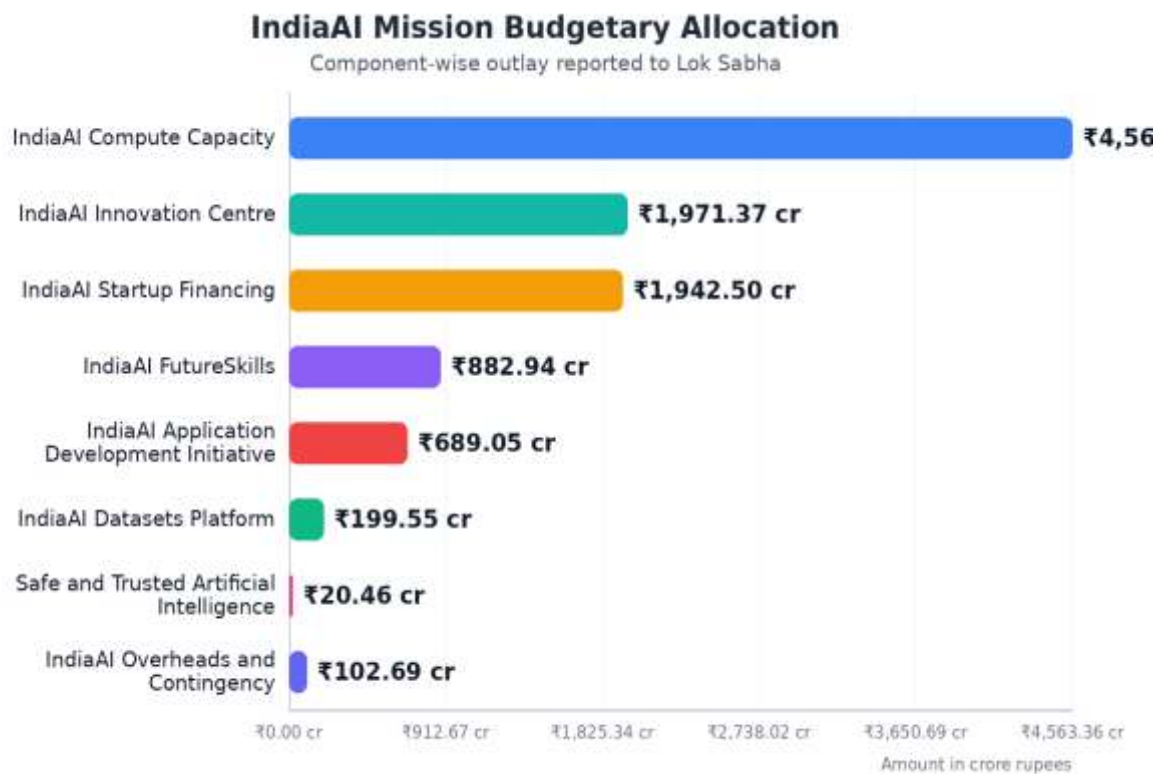


Figure 1. IndiaAI Mission budgetary allocation.²⁷

Figure 1 simplifies comparing needed corporate governance against parliamentary allocation data. Most funding goes towards the domains of Capacity and Innovation, with a smaller portion allocated to the Safe and Trusted Artificial Intelligence domain. This type of allocation indicates that public strategy in India leans more towards ecosystem expansion and less towards the provision and institutionalization of the supervisory, auditing, accountability, risk governance, standards, inter-agency coordination, and enforcement of high-impact Artificial Intelligence in the corporate domain.²⁸

An example of the same imbalance can be seen in the sanction structure of the Digital Personal Data Protection Act, 2023. The largest financial burden is placed in the hierarchy of obligations on the safeguard of security and breach notification, followed by the obligations concerning the protection of children's data and the obligations of Significant Data Fiduciaries. These statutory maxima are represented in Figure 2. The placement comparison is important, as it shows how Indian law defines and locates deterring actions, not in vague ethical constructs,

²⁷ Ministry of Electronics and Information Technology, "India AI Mission" (Lok Sabha Unstarred Question No. 3149, March, 2025).

²⁸ NITI Aayog, "Responsible AI: Part 2 - Operationalizing Principles for Responsible AI" 21 (August, 2021).

but in clear and definable failures of security, notification, and elevated responsibilities of fiduciaries that cannot be delegated.²⁹

Maximum Penalties under the Digital Personal Data Protection Act, 2023

Selected penalty categories relevant to corporate artificial intelligence governance



Figure 2. Maximum penalties under the Digital Personal Data Protection Act, 2023.³⁰

The distribution in Figure 2 captures the extent to which legal requirements create board-level risk exposure and helps analyse governance. Security safeguards and breach notifications are at the top, suggesting that corporations using artificial intelligence will be under statutory pressure to implement operational controls, establish clear escalation paths, and create documented data practices. The failure to meet such statutory requirements is not seen as a breach of governance principles but, rather, a significant enterprise risk, which will likely result in serious financial and reputational harm to the organisation and its leadership.³¹

Principal Regulatory Challenges and Judicial Responses

The challenges of the current framework are revealed when artificial intelligence moves from abstract policy to actual practice. Privacy, market abuses, explanation and evidence

²⁹ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 33.

³⁰ The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), sch. 1.

³¹ Asish K. Bhattacharyya, *Corporate Governance in India: Change and Continuity* 174 (Oxford University Press, New Delhi, 1st edn., 2016).

reconstruction, and vendor dependency show fragmented regulations, and the role of courts and regulators in transforming general duties into governance expectations, are in stark contrast.³²

Privacy, Profiling, and the Constitutional Baseline

The most significant Indian decision at the constitutional level is *Justice K. S. Puttaswamy (Retd.) and Another v. Union of India and Others*³³. The case recognizes privacy as a fundamental right, not only extending to privacy in state databases, but also establishing the normative standard for assessing data collection and extraction, behavioural tracking, and information asymmetry. The case is important for corporate governance because numerous applications of artificial intelligence depend on the extensive and intricate collection and processing of personal data. Even in situations where the immediate question is of legislative scope rather than constitutional, the case considers the intrinsic value of privacy and the digital corporate governance standard.

The most pressing challenge of governance occurs when organisations make profiling 'normal' in the scope and the framework of their business operations, even though they do not explain their purposes for profiling, data retention, or the inferences drawn from use of the data. The challenge is also present in the most recent body of work on artificial intelligence, where it is noted that the governance of artificial intelligence is being addressed in the context of a policy-governance nexus, where transparency, the impact on stakeholders, and the role of regulation coalesce. In the Indian context, this suggests that boards need to look beyond the consent or data usage frameworks and examine the potentially coercive, discriminatory, and structurally exploitative data practices.³⁴

Market Integrity and Automated Trading

Another significant aspect is the reasoning developed in the context of security laws. In *N. Narayanan v. Adjudicating Officer, Securities and Exchange Board of India*³⁵, the protection of investors and preservation of integrity of the market was noted by the Supreme Court to be the essence of the securities laws. There are clear consequences for the governance of artificial

³² Kieron O'Hara, "Explainable AI and the Philosophy and Practice of Explanation", 39 *Computer Law & Security Review* 105474 (2020).

³³ (2017) 10 SCC 1.

³⁴ Cheryl Marie Cordeiro, Laurynas Adomaitis, et.al., "The AI-Policy-Governance Nexus: How Regulation and AI Shift Corporate Governance Toward Stakeholders", 84 *Technology in Society* 103117 (2026).

³⁵ (2013) 12 SCC 152.

intelligence within companies listed on stock exchanges, and within broker, exchange, and advisory firms. Any automated system that alters the basis of recommendations, surveillance, and/or the execution of trades should be assessed from the perspective of the objective of the system of ensuring fairness and transparency in the markets, rather than from the perspective of the efficiency of the system.

This objective is even more apparent in the case of *Securities and Exchange Board of India v. Rakhi Trading Private Limited*³⁶ where the Supreme Court held that synchronized trades and reversal trades, which created a fictitious appearance of market activity, were illegal. Although this case did not deal with today's generative systems, the principle of the case is directly applicable to trading that is driven by algorithms and/or artificial intelligence. The concern of the law is with the distortion of the market, and not with the fact that the distortion is done manually as opposed to done through an automated system. A company may not justify the implementation of a system that is manipulative, by relying on the speed, volume, or lack of transparency of that system.

Data Concentration and Competition Review

The intersection of privacy and competition law is becoming more pronounced with regard to digital markets where AI systems and integration across platforms are reliant upon large datasets. In *WhatsApp LLC v. Competition Commission of India*³⁷, the Delhi High Court ruled that the Competition Commission could proceed with its investigation into WhatsApp's 2021 privacy policy amendment, stating that overlapping issues in law do not imply that a case is outside the scope of investigation. This ruling is relevant for AI governance, as data practices that are consistently employed by firms in a position of structural dominance are recognized as having the potential to raise competition questions.

*Meta Platforms Inc. v. Competition Commission of India and Others*³⁸, decided by the National Company Law Appellate Tribunal in November 2025, further developed this approach. This ruling is of great importance for corporate governance, as it acknowledges the need for a synergistic analysis of privacy-based data sharing and the abuse of market-dominance from a competition law perspective, as opposed to analysing them in isolation. For firms considering the integration of AI within corporate ecosystems, the interpretation of governance failures

³⁶ (2018) 13 SCC 753.

³⁷ 2022 SCC OnLine Del 2582.

³⁸ Competition Appeal (AT) No. 2 of 2025, National Company Law Appellate Tribunal, judgment dated November 4, 2025.

within corporate ecosystems is that the failure to design data governance controls adequately will expose the firm to competition law claims.

Evidence, Explainability, and Organisational Design

Proof is another challenge. If a harmful outcome is caused by a decision taken using a workflow supported by artificial intelligence, regulators, and courts will have to decide whether the related failure is due to model design, choice of training data, human intervention, supervision, procurement, or implementation. Perry Keller and Archie Drake have legitimately warned that if institutions believe that technical standards will resolve issues of accountability, explainable artificial intelligence will become both exclusionary and paternalistic. In the corporate world, the evidentiary issue is further complicated by redundant decision-making processes and layers of software and cloud service providers, consultants, internal staff, and management.³⁹

Indian governance practice, therefore, demands a greater organisational response than procurement due diligence. Boards should require the provision of model inventories, escalation matrices, validation logs, and minutes that record the review of significant artificial intelligence outputs prior to adoption. Recent legal research on digital corporate governance further reinforces the need for corporate law to create structures that cater for the data economy, in which decision-making and control processes are increasingly facilitated through digital constructs. In the absence of documented testing, oversight, and the right of control to intervene, what appears to be a sound legal defence for implementation may easily become commercially indefensible in the event of litigation for discrimination, a breach, manipulation, or unjust exclusion.⁴⁰

Conclusion

While current Indian corporate law contains an adequate amount of statutory provisions and mechanisms for controlling corporate artificial intelligence, these provisions and mechanisms are scattered across multiple laws, regulatory authorities, and adjudicatory bodies. The question, therefore, is not whether laws are applicable, but whether the existing legal framework can truly capture the phenomenon and be used with enough consistency and coherence to match the growing pace of corporate innovation.⁴¹

³⁹ Perry Keller and Archie Drake, "Exclusivity and Paternalism in the Public Governance of Explainable AI", 40 *Computer Law & Security Review* 105490 (2021).

⁴⁰ Florian Möslein, "European Company Law in the Age of Digital Transformation: Artificial Intelligence, Data Economy, and Digital Corporate Governance", 26 *ERA Forum* 629 (2025).

⁴¹ Karen Yeung and Martin Lodge, *Algorithmic Regulation* 93 (Oxford University Press, Oxford, 1st edn., 2019).

This paper has argued that, in the context of Indian law, artificial intelligence should be seen as a governance object rather than as an instrument of production that is neutral. When artificial intelligence becomes part of reporting, compliance, customer analytics, trading systems, or board support systems, it influences the way a company distributes its resources, including information, risk, and accountability. The existing provisions of the Companies Act, 2013, the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and laws concerning the regulation of securities and competition law, already provide an adequate framework of basic principles. What they do not provide, and what is needed, is a consistent framework of institutional provisions for attribution, explanation, and cooperation among regulatory bodies.⁴²

The emerging trend of judging privacy and integrity of the market, as well as the coercive nature of data practices by Indian courts, is still somewhat progressive. Although new technologies may make some aspects of the law complex and difficult to interpret, sector-based regulators have shifted from a position of passive observation to a position of structured coping, especially in the areas of securities and cyber governance. In this regard, Indian laws will not recognize any broad-based immunity for automated corporate decision-making. This is also true in the context of the coercive nature of artificial intelligence and automated corporate decision-making. Indian courts will progressively evaluate the coercive nature of artificial intelligence in the context of adequate assurance, the fairness of data practices and firm's ability to recreate and substantiate significant decisions.⁴³

The challenge now is more a matter of the design of the firm's governance systems to address the regulatory context, rather than the design of new legal doctrines. To fulfill the existing legal requirements, Indian corporate governance will require more than just artificial intelligence charters that are approved by the boards, guaranteed integrity across the supply chain, and controlled practices of greater predictability across disparate sectors. These may be achieved through an artificial intelligence law. The existing legal frameworks demand of corporate governance systems that boards of organisations recognize artificial intelligence as a latent and delegated source of governance control that is both visible and accountable to the firm's legal

⁴² Michael Hilb, "Toward Artificial Governance? The Role of Artificial Intelligence in Shaping the Future of Corporate Governance", 24 *Journal of Management and Governance* 851 (2020).

⁴³ Cheryl Marie Cordeiro, Laurynas Adomaitis, et.al., "The AI-Policy-Governance Nexus: How Regulation and AI Shift Corporate Governance Toward Stakeholders", 84 *Technology in Society* 103117 (2026).

governance order.⁴⁴

Suggestions

In the Indian regulations presented in this study, reforms should be grounded in the reality of organisational oversight of artificial intelligence that is auditable and aimed at regulators, rather than being aspirational. The following suggestions target boards, compliance teams, and regulators, as well as listed companies with a focus on market and data sensitive artificial intelligence systems.

1. Adopt board-level artificial intelligence charters: All companies implementing significant artificial intelligence systems should have a charter, approved by the board, defining approval limits, acceptable uses, and obligations to document and escalate. Low-risk automation should be differentiated from systems that impact disclosure, employment, treatment of consumers, pricing, or market behaviour.
2. Create mandatory model inventories: Corporations should keep a current account of all AI and machine learning tools employed in governance, compliance, customer-facing, and market-facing applications. This account should detail the system's purpose, vendor, and training; indicate the source of data and its validation; specify who has override authority; and outline relevant legal frameworks.
3. Link artificial intelligence review to Section 166 duties: Documents for the board's consideration must explain how proposed AI solutions observe the duties of care, diligence, good faith, and independent judgment as prescribed in the Companies Act, 2013. This will help to shift from vague fiduciary duties to an accountable system of governance and will curtail the practice of treating automation as a managerial black box.
4. Strengthen audit committee supervision: Audit committees are required to provide oversight over model validation, data-quality control, incident reports, and the impact of AI on internal financial control systems. Where an automated system materially impacts reporting, risk flags, or fraud detection, the committee should obtain periodic assurance from management and the internal audit function.
5. Mandate explainability records for consequential decisions: Organisations are required to maintain concise and digestible AI explainability records pertaining to systems that

⁴⁴ Bob Tricker, *Corporate Governance: Principles, Policies, and Practices* 242 (Oxford University Press, Oxford, 5th edn., 2025).

materially influence the enforcement of legal rights, the outcome of investor communications, employment decisions, or compliance determinations. The primary focus is not on fully technical detail in every instance, but rather explainability that can be audited pertaining to the limits, inputs, review, and justification of trust.

6. Integrate data protection impact assessments with enterprise risk management: For high-impact systems, data protection reviews should be incorporated into the overall enterprise risk management framework, instead of being treated as a stand-alone privacy checklist. This inclusion enables boards to assess the risks associated with profiling, potential breaches, retention rationale, issues concerning children's data, and the harm caused to downstream stakeholders, all within the same governance framework.
7. Impose stricter vendor accountability clauses: AI procurement contracts should include logging requirements, validated data, breach support, access to audits, assistance with bias testing, and the assumption of risk. If these contractual provisions are not present, the company retains governance risk while being unable to exercise any oversight.
8. Develop sector-specific disclosure standards: The Securities and Exchange Board of India needs to replace the consultative approach with incremental disclosure standards for listed companies and regulated intermediaries employing material artificial intelligence systems. The focus of disclosure should be on use-case and governance safeguards, human intervention, testing, and incident management, as opposed to the proprietary technologies.
9. Coordinate data protection, cyber, and competition enforcement: Governments should establish structured consultation or referral mechanisms when data practices, cybersecurity incidents, and market dominance converge. The majority of artificial intelligence disputes occur at the intersection of multiple regulatory domains. Consequently, fragmented enforcement will result in significant governance failures, which may seem less important from the perspective of a single regulatory framework.
10. Build adjudicatory capacity on technical evidence: Regulators and tribunals should define their expectations for model logs, validation records, prompt histories, and override documentation. A more distinct evidentiary framework would enhance the quality of enforcement and potentially motivate firms to maintain governance records proactively, as opposed to retroactively, before legal disputes emerge.

Bibliography

Books:

- Asish K. Bhattacharyya, Corporate Governance in India: Change and Continuity (Oxford University Press, New Delhi, 1st edn., 2016).
- Bob Tricker, Corporate Governance: Principles, Policies, and Practices (Oxford University Press, Oxford, 5th edn., 2025).
- Karen Yeung and Martin Lodge, Algorithmic Regulation (Oxford University Press, Oxford, 1st edn., 2019).
- Reinier Kraakman, John Armour, et.al., The Anatomy of Corporate Law: A Comparative and Functional Approach (Oxford University Press, Oxford, 3rd edn., 2017).
- Woodrow Barfield and Ugo Pagallo, Research Handbook on the Law of Artificial Intelligence (Edward Elgar Publishing, Cheltenham, 2nd edn., 2025).

Statutes:

- The Companies Act, 2013 (Act No. 18 of 2013).
- The Competition Act, 2002 (Act No. 12 of 2003).
- The Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities (REs), 2024 (SEBI Circular No. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2024/113).
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
- The Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet, 2022 (No. 20(3)/2022-CERT-In).
- The Information Technology Act, 2000 (Act No. 21 of 2000).
- The Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Market Infrastructure Institutions (MIIs), 2019 (SEBI Circular No. SEBI/HO/MRD/DOP1/CIR/P/2019/24).
- The Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by market intermediaries, 2019 (SEBI Circular No. SEBI/HO/MIRSD/DOS2/CIR/P/2019/10).

- The Reporting for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used by Mutual Funds, 2019 (SEBI Circular No. SEBI/HO/IMD/DF5/CIR/P/2019/63).
- The Securities and Exchange Board of India Act, 1992 (Act No. 15 of 1992).
- The Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 (Notification No. SEBI/LAD-NRO/GN/2015-16/013).

Reports:

- Ministry of Electronics and Information Technology, "India AI Mission" (Lok Sabha Unstarred Question No. 3149, March, 2025).
- NITI Aayog, "National Strategy for Artificial Intelligence #AIForAll" 11 (June, 2018).
- NITI Aayog, "Responsible AI: Approach Document for India, Part 1: Principles for Responsible AI" 18 (February, 2021).
- NITI Aayog, "Responsible AI: Part 2 - Operationalizing Principles for Responsible AI" 21 (August, 2021).
- Securities and Exchange Board of India, "Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets" (June, 2025).

Articles:

- Cheryl Marie Cordeiro, Laurynas Adomaitis, et.al., "The AI-Policy-Governance Nexus: How Regulation and AI Shift Corporate Governance Toward Stakeholders", 84 Technology in Society 103117 (2026).
- Florian Möslein, "European Company Law in the Age of Digital Transformation: Artificial Intelligence, Data Economy, and Digital Corporate Governance", 26 ERA Forum 629 (2025).
- Kieron O'Hara, "Explainable AI and the Philosophy and Practice of Explanation", 39 Computer Law & Security Review 105474 (2020).
- Michael Hilb, "Toward Artificial Governance? The Role of Artificial Intelligence in Shaping the Future of Corporate Governance", 24 Journal of Management and Governance 851 (2020).
- Perry Keller and Archie Drake, "Exclusivity and Paternalism in the Public Governance of Explainable AI", 40 Computer Law & Security Review 105490 (2021).

- Rowena Rodrigues, "Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities", 4 Journal of Responsible Technology 100005 (2020).

Websites:

- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2012355>

