INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

REGULATORY GAPS FOR AI-ASSISTED INSIDER THREATS & "SHADOW AI" IN CORPORATE GOVERNANCE

AUTHORED BY - MERBIN T D

ABSTRACT

The exponential adoption of artificial intelligence (AI) in organizational environments has created both unprecedented opportunities and emergent threats. Among these, AI-assisted insider threats and Shadow AI, the unsanctioned or unmanaged use of AI systems by employees pose serious governance, compliance, and ethical challenges. This paper examines the regulatory vacuum surrounding these phenomena, focusing primarily on India while drawing comparative insights from the European Union and the United States. It explores how existing data protection, cybersecurity, and corporate governance frameworks fail to address the complex accountability and transparency issues triggered by autonomous and semi-autonomous AI systems. Through doctrinal and comparative analysis, this paper identifies gaps in India's legal infrastructure, particularly in relation to data stewardship, fiduciary duties of directors, and enforcement under the Information Technology Act, 2000 and Digital Personal Data Protection Act, 2023.

INTRODUCTION

Artificial intelligence (AI) has rapidly evolved from a tool of computational efficiency to an indispensable element in global business infrastructure. From predictive analytics to automated decision-making, AI systems now underpin corporate governance, compliance, and data management frameworks. However, as organizations race to integrate AI technologies, new and largely unregulated risks have emerged. Among these are AI-assisted insider threats instances where employees or internal actors leverage AI systems for unauthorized or harmful purposes and Shadow AI, the deployment of unapproved AI applications within enterprises without the knowledge or consent of information technology (IT) or compliance departments. The convergence of these two risks presents a formidable challenge to data governance and corporate accountability. Shadow AI undermines oversight and compliance, while AI-assisted insider threats exploit the opacity and autonomy of algorithmic systems to manipulate,

ISSN: 2582-6433

exfiltrate, or misuse corporate data. Together, they reveal critical deficiencies in existing regulatory and corporate governance frameworks, particularly in jurisdictions such as India, where AI-specific legal standards are nascent and fragmented. While the European Union (EU) has introduced a comprehensive Artificial Intelligence Act (AI Act) to establish risk-based governance mechanisms, and the United States relies on a mixture of sectoral regulations and self-regulatory guidance, India remains at a formative stage. The Indian legal landscape is defined by general statutes such as the Information Technology Act, 2000 (IT Act) and the Digital Personal Data Protection Act, 2023 (DPDP Act), neither of which adequately contemplates the complexities of autonomous or semi-autonomous AI behavior. This article argues that the regulatory lacuna surrounding AI-assisted insider threats and Shadow AI undermines the principles of transparency, accountability, and fiduciary duty central to corporate governance. It contends that AI systems, when unregulated, create a "double agency problem": they act as both tools and potential independent actors, distorting the conventional boundaries of liability between corporate entities, employees, and directors. To address this vacuum, the paper adopts a comparative legal approach.

UNDERSTANDING SHADOW AI AND AI-ASSISTED INSIDER THREATS

A. The Concept of Shadow AI

Shadow AI refers to the unsanctioned or unmanaged use of AI systems within an organization, analogous to the phenomenon of Shadow IT where employees deploy unapproved software or hardware for business purposes. In the context of AI, Shadow AI encompasses generative models, natural language processing tools, and data analysis algorithms adopted without authorization or oversight. These may include publicly accessible tools such as ChatGPT, Midjourney, or Bard, integrated into workflows without compliance vetting. Employees may, for example, use generative AI tools to draft business proposals, analyze client data, or generate code all of which might involve the transfer of proprietary or personally identifiable information (PII) to third-party platforms. Such behavior, though often motivated by productivity gains, introduces substantial security vulnerabilities. Unauthorized AI tools can store, process, or replicate sensitive data, thereby breaching confidentiality obligations and data protection laws. A recent report by Microsoft and LinkedIn (2024) revealed that nearly 75% of global knowledge workers now use generative AI tools in some capacity, often without explicit

ISSN: 2582-6433

employer authorization.[1] This unregulated adoption heightens exposure to data leaks, intellectual property infringement, and regulatory non-compliance.

B. The Nature of AI-Assisted Insider Threats

An AI-assisted insider threat arises when a legitimate user typically an employee or contractor leverages AI systems to carry out malicious or negligent activities within an organization. Such threats differ from traditional insider attacks in that they exploit AI's capacity for autonomous learning, data aggregation, and predictive analytics. For instance, an employee might manipulate an AI-based data analytics tool to obscure financial irregularities, or use generative AI to create realistic but falsified documents. In other cases, AI chatbots integrated into corporate systems could be exploited to extract sensitive information via prompt injection or data manipulation techniques. In regulatory terms, insider threats of this nature blur the line between human agency and algorithmic autonomy. The human actor initiates the behavior, but the AI system amplifies its scope and impact. Current legal frameworks built upon anthropocentric notions of intent and control struggle to assign liability in such hybrid scenarios.

C. Interrelation Between Shadow AI and Insider Threats

Shadow AI often functions as an enabler of AI-assisted insider threats. When employees adopt unsanctioned AI tools, they circumvent established governance mechanisms such as data access controls, encryption standards, and audit trails. This lack of visibility prevents compliance teams from identifying risky data flows or unauthorized model training activities. Moreover, Shadow AI increases exposure to "data drift" and "model poisoning" where external AI systems trained on corporate data produce skewed or biased outputs, potentially influencing internal decision-making. In corporate governance terms, this constitutes a breach of directors' duties to exercise due diligence and prudence in safeguarding the company's assets and information. The dual emergence of Shadow AI and AI-assisted insider threats thus necessitates a re-examination of governance principles, emphasizing the intersection of technological risk and fiduciary responsibility.

D. Corporate Exposure and Reputational Risk

From a corporate governance standpoint, the proliferation of Shadow AI undermines the

[1]Microsoft & LinkedIn, 2024 Work Trend Index Annual Report (2024).

ISSN: 2582-6433

internal control environment central to compliance. Board oversight mechanisms, risk committees, and audit functions traditionally rely on transparent data management. Unmonitored AI activity disrupts this visibility, creating potential violations of securities law disclosures and data protection obligations. Reputationally, organizations face heightened scrutiny from regulators and investors. A single data breach arising from unauthorized AI usage can lead to enforcement under data protection statutes or class-action litigation for breach of fiduciary duty. Companies such as Samsung and JPMorgan have already imposed internal bans on generative AI tools after employees inadvertently exposed sensitive information.[2] Therefore, addressing Shadow AI and AI-assisted insider threats is not merely a matter of technological hygiene but a cornerstone of sustainable corporate governance.

THE LEGAL AND REGULATORY FRAMEWORK: INDIA, THE EU, AND THE UNITED STATES

A. The Indian Regulatory Context

India's engagement with artificial intelligence governance remains at an early stage. While the Digital Personal Data Protection Act, 2023 (DPDP Act) and the Information Technology Act, 2000 (IT Act) offer broad frameworks for data privacy and cybersecurity, neither statute directly regulates AI systems or the risks posed by Shadow AI. Under the DPDP Act, data fiduciaries must process personal data in a "lawful and fair manner" and implement "reasonable security safeguards" to prevent data breaches.[3] However, these obligations are directed toward data processing entities rather than algorithmic systems themselves. Shadow AI, which operates outside sanctioned corporate channels, thus falls beyond the explicit purview of compliance monitoring. The IT Act, supplemented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, focuses primarily on intermediary liability and data protection.[4] Its framework assumes identifiable control and traceability assumptions incompatible with autonomous or semi-autonomous AI systems that learn and evolve through data exposure. The absence of a dedicated AI regulatory instrument leaves critical questions unresolved:

- Who bears liability when an AI system independently causes harm or data leakage?
- How can corporate boards discharge their fiduciary duties when internal AI usage is

[2] Reuters, "Samsung Bans Generative AI Tools After Data Leaks," Reuters Technology (May 2023).
[3] Digital Personal Data Protection Act, No. 22 of 2023, § 8 (India).
[4] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

ISSN: 2582-6433

opaque?

- What compliance mechanisms can ensure AI systems align with corporate ethics and legal obligations?

To date, the Indian government's approach has been largely policy-driven rather than legislative. The NITI Aayog's National Strategy for Artificial Intelligence (2018) emphasizes "AI for All" as a developmental priority but omits enforceable governance standards.[5] The Ministry of Electronics and Information Technology (MeitY) has signaled its intention to introduce an AI-specific framework, but as of 2025, regulatory proposals remain under consultation. This leaves corporations in a self-regulatory vacuum dependent on internal ethics committees, data protection officers, and voluntary compliance programs to manage AI-related risks. However, without statutory backing, such mechanisms lack enforceability, rendering them vulnerable to conflicts of interest and underreporting.

B. The European Union: Rights-Based Regulation

In contrast, the European Union has taken a comprehensive, risk-based approach through the Artificial Intelligence Act (EU AI Act). This legislation categorizes AI applications into four risk tiers unacceptable, high, limited, and minimal imposing proportional compliance obligations on developers and deployers. The AI Act mandates transparency, human oversight, and data governance for high-risk AI systems. It explicitly prohibits manipulative or discriminatory AI applications and integrates its provisions with the General Data Protection Regulation (GDPR). For corporations operating within the EU, this framework effectively closes many of the gaps that allow Shadow AI to proliferate. Notably, Article 10 of the AI Act requires organizations to implement data governance measures ensuring the quality, relevance, and representativeness of datasets used in model training. This provision directly addresses risks associated with unsanctioned model deployment or unvetted data inputs the hallmarks of Shadow AI. Furthermore, Article 29 imposes post-market monitoring obligations, compelling organizations to establish traceability mechanisms for AI outputs. This facilitates auditability, enabling regulators to determine whether a breach originated from authorized or unauthorized AI use. While the EU model is regulatory-heavy, it provides a clear blueprint for balancing innovation with accountability. For India, adapting similar risk-tiered compliance could harmonize AI governance with global standards while accommodating local socio-economic contexts.

[5] NITI Aayog, National Strategy for Artificial Intelligence #AIforAll (2018).

ISSN: 2582-6433

C. The United States: Sectoral and Corporate Governance Approach

The United States lacks a unified federal statute on AI, opting instead for a mosaic of sectoral regulations and corporate governance standards. Agencies such as the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and National Institute of Standards and Technology (NIST) each exercise partial oversight over AI-related risks. The NIST AI Risk Management Framework (AI RMF) promotes principles of transparency, accountability, and explainability in AI systems. Although nonbinding, it serves as the de facto standard for corporate AI governance, particularly within data-sensitive industries. The FTC, leveraging its authority under Section 5 of the Federal Trade Commission Act, has pursued enforcement actions against companies that deploy AI systems misleadingly or insecurely. In In re Everalbum, Inc., the FTC held that a company's failure to delete facial recognition data upon user request constituted an unfair practice, signaling that algorithmic opacity could amount to consumer deception. Meanwhile, corporate law scholars argue that AI governance aligns with directors' fiduciary duties of care and loyalty under Delaware General Corporation Law. Board oversight failures relating to algorithmic risk management could therefore attract derivative liability under the Caremark doctrine. The U.S. model thus integrates AI accountability through existing legal doctrines rather than standalone legislation. While flexible, this approach risks under-enforcement in areas like Shadow AI, where unauthorized use may escape corporate awareness until after harm occurs.

D. Comparative Synthesis

Comparatively, India's absence of AI-specific statutes places it closer to the U.S. model in reliance on soft law and corporate governance principles, but without the institutional depth of enforcement agencies like the FTC or NIST. Conversely, the EU's codified approach offers strong legal certainty but may impose heavy compliance burdens unsuited to emerging markets. A balanced path for India lies in integrating the rights-based safeguards of the EU model particularly transparency and risk classification with the flexibility of the U.S. self-regulatory system. Embedding such obligations within the DPDP Act's data fiduciary framework could provide statutory grounding while leveraging corporate accountability mechanisms to detect and mitigate Shadow AI risks.

CORPORATE GOVERNANCE IMPLICATIONS AND LIABILITY

A. Fiduciary Duties in the Age of Artificial Intelligence

Corporate governance rests on the fiduciary duties of directors and officers principally the duty

ISSN: 2582-6433

of care, duty of loyalty, and duty to act in good faith.[6] These duties, codified in Indian corporate jurisprudence through the Companies Act, 2013 and interpreted in cases such as Tata Consultancy Services Ltd. v. Cyrus Investments Pvt. Ltd.,[7] demand that directors exercise due diligence in overseeing corporate operations. In the AI context, these duties extend to the adoption, monitoring, and supervision of algorithmic systems. When directors permit or ignore the proliferation of Shadow AI within their organization, they effectively abdicate oversight of a material operational risk. The failure to establish internal controls for AI governance can thus constitute a breach of the duty of care. Moreover, AI-assisted insider threats challenge the contours of the business judgment rule the principle shielding directors from liability for informed business decisions made in good faith.[8] Decisions taken without understanding the technological implications of AI tools cannot qualify as "informed." Boards are therefore obligated to ensure that AI adoption is accompanied by adequate risk assessments, ethical guidelines, and compliance reviews. This fiduciary expansion aligns with the evolving doctrine of algorithmic accountability, which requires directors to ensure that automated systems do not compromise legal or ethical standards.[9] Corporate boards must, therefore, maintain continuous oversight over AI systems throughout their lifecycle from procurement to deployment and post-deployment monitoring.

B. Internal Controls and Compliance Programs

Internal control mechanisms serve as the backbone of corporate governance. The proliferation of Shadow AI undermines these controls by creating unmonitored entry points for data processing and storage. Traditional compliance programs centered on manual audits or static risk matrices are insufficient to manage dynamic AI environments. To counter this, organizations must implement AI-specific compliance architectures incorporating:

1. Algorithmic Audit Trails – Systems that record every AI decision, data source, and modification for traceability.
2. Access and Usage Controls – Role-based permissions for AI tool deployment to prevent unsanctioned use.
3. Model Governance Frameworks – Policies ensuring dataset integrity, bias testing, and ethical use of generative models.

[6] Companies Act, No. 18 of 2013, § 166 (India)
[7] Tata Consultancy Servs. Ltd. v. Cyrus Investments Pvt. Ltd., (2021) 9 SCC 449 (India).
[8] Aronson v. Lewis, 473 A.2d 805 (Del. 1984).
[9] Karen Yeung, Algorithmic Regulation: A Critical Interrogation, 12 Reg. & Governance 505 (2018).

ISSN: 2582-6433

4. Incident Response Protocols – Procedures for investigating data leaks or manipulation arising from AI misuse.

In India, the Securities and Exchange Board of India (SEBI) has emphasized the importance of internal controls under Regulation 17(8) of the Listing Obligations and Disclosure Requirements (LODR) Regulations, 2015.[10] Extending these controls to encompass AI governance would enhance board accountability and investor confidence. Globally, the OECD Principles of Corporate Governance (2023) encourage boards to consider "technological and cybersecurity risks" within their governance purview. AI systems fall squarely within this mandate, necessitating their inclusion in corporate risk registers.

C. Attribution of Liability

One of the most complex challenges in regulating AI-assisted insider threats lies in the attribution of liability. When AI systems operate autonomously or semi-autonomously, determining whether culpability lies with the employee, the corporation, or the AI developer becomes intricate. Under Indian law, the doctrine of vicarious liability holds corporations responsible for the acts of their agents performed in the course of employment. However, this presupposes human agency and intent both of which are blurred in the case of AI-driven conduct. When an employee deploys a generative AI tool that independently disseminates confidential data, attributing fault solely to the employee may be legally insufficient. Courts may instead examine whether the corporation exercised adequate due diligence in monitoring internal AI usage. The absence of policy frameworks, monitoring systems, or employee training could render the organization liable under both corporate and data protection laws. In the European Union, Article 71 of the AI Act imposes administrative fines on deployers who fail to ensure AI compliance, regardless of whether violations were intentional or negligent. Similarly, in the United States, the FTC has held organizations accountable for the downstream consequences of algorithmic bias, even where such bias arose from autonomous model behavior. India, by contrast, lacks explicit precedent on algorithmic liability. The IT Act and DPDP Act impose data fiduciary obligations but do not clarify whether directors or compliance officers can be held personally liable for AI misconduct. Introducing strict liability provisions for corporate AI governance could thus fill a critical enforcement gap.

[10] SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015, Reg. 17(8).

ISSN: 2582-6433

D. AI Risk Governance at the Board Level

Modern corporate governance increasingly requires that boards adopt a technology stewardship role. Boards must not only ensure compliance but also integrate AI ethics into strategic decision-making. This entails: Establishing AI Oversight Committees comprising directors, data scientists, and legal officers; Mandating periodic AI Risk Reports for disclosure to shareholders; Integrating AI governance into Environmental, Social, and Governance (ESG) metrics; and Ensuring that third-party AI vendors adhere to equivalent data protection and ethical standards. The Institute of Company Secretaries of India (ICSI), in its 2024 guidance note on digital governance, recommends that boards conduct periodic evaluations of algorithmic systems to ensure compliance with the DPDP Act and global best practices. In the EU, large corporations are already required under the Corporate Sustainability Reporting Directive (CSRD) to disclose how emerging technologies, including AI, impact their risk and governance strategies. Adoption of similar disclosure norms in India would enhance transparency and align domestic corporations with global investors' expectations. Ultimately, AI governance must be treated not as an auxiliary compliance issue but as an integral component of fiduciary governance, reflecting the growing interdependence between technology, ethics, and corporate accountability.

ADDRESSING REGULATORY GAPS AND EMERGING POLICY CHALLENGES

A. Fragmented Legal Architecture

India's legal framework for emerging technologies remains largely reactive and sector-driven. The Information Technology Act, 2000 was drafted in a pre-AI era and focuses primarily on cybercrimes, electronic records, and intermediary liability. The Digital Personal Data Protection Act, 2023 (DPDP Act) modernizes privacy law but omits explicit references to artificial intelligence, algorithmic profiling, or automated decision-making. Consequently, the two principal statutes governing the digital ecosystem fail to create a coherent AI liability regime. This fragmentation manifests in three dimensions. First, jurisdictional ambiguity whether AI-related misconduct constitutes a data-protection violation, a cybersecurity lapse, or a corporate-governance breach is unresolved. Enforcement agencies such as the Indian Computer Emergency Response Team (CERT-In) and the Data Protection Board have overlapping but undefined authority. Second, accountability diffusion arises because AI deployment often involves multiple entities developers, vendors, and end-users. Absent

ISSN: 2582-6433

statutory allocation of responsibility, each can disclaim liability for harm. Third, there is regulatory inertia. While the NITI Aayog's Responsible AI initiative articulates ethical principles such as fairness and transparency, these remain policy aspirations without binding force. The cumulative effect is a compliance vacuum in which Shadow AI flourishes. Corporations can neither be penalized effectively for unauthorized AI use nor claim a clear safe-harbor for good-faith deployment.

B. Data Governance and Algorithmic Transparency

A central regulatory gap concerns algorithmic transparency. The DPDP Act requires that data fiduciaries inform data principals of processing purposes, yet it does not extend this duty to automated decisions made by AI systems. In contrast, Article 22 of the GDPR guarantees individuals the right to human review of automated decisions. Lack of transparency undermines both due-process rights and corporate accountability. When AI tools process personal or proprietary data without clear audit trails, it becomes impossible for regulators or even boards to determine whether a breach resulted from Shadow AI or sanctioned activity. India's Reserve Bank of India (RBI) has expressed concern over algorithmic credit scoring in its Guidelines on Digital Lending, 2022, emphasizing explainability in AI models. However, these guidelines apply narrowly to financial intermediaries. A broader cross-sectoral transparency obligation similar to the EU's AI Act remains absent.

C. Cross-Border Data Transfers and AI Supply Chains

Another lacuna lies in regulating cross-border data flows in AI development. Generative-AI models often rely on global datasets processed through cloud-based infrastructure located outside India. While Section 16 of the DPDP Act authorizes the government to restrict transfers to certain jurisdictions, it does not impose due-diligence obligations on data exporters to ensure that foreign AI vendors comply with Indian privacy norms. The absence of reciprocal enforcement mechanisms exposes Indian corporations to jurisdictional risk: data exfiltrated by Shadow AI tools hosted abroad may fall outside the reach of Indian regulators. By contrast, the EU employs adequacy decisions and standard contractual clauses under the GDPR to ensure cross-border accountability.[11] India could adopt a similar mechanism through bilateral digital-trade agreements or an AI Safe-Harbor Certification Scheme, requiring foreign vendors to demonstrate compliance with domestic standards before processing Indian data.

[11] GDPR, supra note 7, arts. 45–47.

ISSN: 2582-6433

D. Ethical and Societal Considerations

Beyond legal deficiencies, the absence of a normative AI ethics framework exacerbates the governance deficit. AI systems can perpetuate bias, discrimination, and misinformation issues particularly salient in a diverse society like India. Without ethical benchmarks, corporate decision-making risks privileging efficiency over equity. Scholars have urged the adoption of a "human-in-command" principle, ensuring that ultimate decision-making authority rests with human agents. Embedding such principles in corporate codes of conduct would reaffirm the moral agency of boards and employees alike. Ethical AI governance also intersects with corporate social responsibility (CSR). Section 135 of the Companies Act, 2013 could be interpreted to include technology ethics initiatives such as AI-literacy programs and algorithmic-bias research within permissible CSR activities, thereby aligning innovation with social accountability.

E. Emerging Policy Challenges

India's forthcoming Digital India Act, expected to replace the IT Act, presents an opportunity to codify AI governance. Early consultation papers suggest inclusion of provisions on algorithmic accountability, consent management, and deep-fake regulation.[12] However, unless the statute also addresses internal corporate use of AI including Shadow AI it will fall short of comprehensive oversight. Policymakers must also grapple with the balance between innovation and regulation. Over-regulation may stifle startups and deter investment; under-regulation risks systemic data breaches. A tiered compliance framework, akin to the EU's risk-based model, could reconcile these interests by calibrating obligations to the risk level of each AI application. Finally, India faces a shortage of AI-literate legal professionals and regulators. Building capacity through interdisciplinary education integrating law, ethics, and data science will be crucial to sustainable AI governance.

CONCLUSION

Artificial intelligence has transformed the operational and strategic dimensions of modern enterprises. Yet, the unregulated rise of Shadow AI and AI-assisted insider threats poses significant challenges to traditional governance paradigms. India's current legal framework anchored in the IT Act and DPDP Act remains insufficient to address these hybrid risks. Without statutory clarity, corporations face uncertainty regarding liability, compliance, and

[12] Ministry of Electronics & Info. Tech., Digital India Act Consultation Paper (2024).

ISSN: 2582-6433

ethical responsibility. This paper argues that the solution lies in hybrid governance: combining statutory precision with corporate self-regulation. A dedicated AI Regulation Act, supported by institutional reforms and corporate accountability mechanisms, would ensure that innovation proceeds within a robust legal and ethical architecture. By integrating AI governance into the core of fiduciary oversight, India can position itself not merely as a consumer of global AI systems but as a normative leader in responsible technological regulation. The future of corporate governance will hinge not on whether AI is adopted but on whether it is governed wisely.