VOLUME 7 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

AUTOMATED VIGIL MECHANISMS: EVALUATING AI-DRIVEN WHISTLEBLOWING FRAMEWORKS UNDER INDIAN CORPORATE LAW

- Chirag Bhoot[1] & Muskan Agarwal[2]

Abstract

This study aims at carrying out an analysis of the efficacy of the automated vigil mechanism in relation to Indian Corporate Law. Whistleblower protections governed by Section 177 of the Companies Act, 2013 and SEBI (LODR) Regulations are traditionally manual reporting procedures. By incorporating artificial intelligence tools, such as NLP technology, Machine Learning algorithms and predictive scoring systems, the process can be made more efficient by ensuring constant monitoring and anonymity. However, there are several legal issues which arise due to the use of algorithms such as bias, opaque scoring, ensuring that personal data regulations contained within the Digital Personal Data Protection Act, 2023 are complied with and evidential issues under the Bharatiya Sakshya Adhiniyam, 2023. In addition, under Section 166 statutory duty cannot be delegated therefore the company board cannot delegate the monitoring processes to an automated system. Therefore, this study recommends a balanced approach to regulation by enforcing mandatory algorithmic monitoring, tamper-proof audit trails and strict "Human-in-the-Loop" processes monitored by Audit Committees.

Keywords: *Bharatiya Sakshya Adhiniyam; SEBI; Audit Committees; Digital Personal Data Protection Act.*

[1]4th Year, B.A.,LL.B.(H), Amity University Kolkata
[2]4th Year, B.A.,LL.B.(H), Amity University Kolkata

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

© 2026 International Journal of Advanced Legal Research

1. Introduction

1.1 The Evolution of Corporate Transparency and Whistleblowing

Corporate governance has become a highly integral part to companies in modern day society. In traditional corporate governance transparency was achieved with limited reporting and regular audits. Whistleblowers could also report any issues they had, relating to financial misconduct, ethical and legal issues, within a company by using the traditional methods. These usually include an email address, drop box and/or external hotline. Individuals are often discouraged from taking the step of whistleblowing due to fear of facing repercussions at work, being blacklisted, having confidential information leaked and delays caused by humans investigating the issue. This can result in serious issues being missed within the company such as accounting manipulation and serious legal issues.[3]

1.2 Defining Automated Vigil Mechanisms

An automated monitoring system is an advanced system incorporating company policy and using AI technology. The automated systems include secure portals with encryption which will use natural language processing to identify, remove any personal details such as IP addresses, time of speech, unique words and forward onto the correct oversight body such as the Audit Committee.

In engineering intensive companies such as listed IT service and product engineering companies like Mindteck (India) Limited, automated monitoring systems are used to review financial transactions, internal audit records, procurement charging and system weaknesses. By reviewing high risk scenarios, ensuring intercompany transactions are correct and reviewing vendor data against legal requirements automated alert systems can help with the internal audit function.[4]

1.3 Technological Disruption vs. Legal Paradigms

[3] Ramya, E. (2026). Whistleblower Protection and Corporate Governance in India: A Critical Analysis of the Effectiveness of the Vigil Mechanism. *International Journal of Legal Science and Innovation*, *8*(1), 1-14.https://doi.org/10.63108/IJLSI.7005

[4] Government of India — Digital Personal Data Protection Act, 2023: Cyber Laws India Official Text Portal

© 2026 International Journal of Advanced Legal Research

This has led to a serious conflict between the traditional concepts of law and the new AI Compliance tools. Indian Corporate Law is governed mainly by the Companies Act, 2013 and various rules made by the SEBI. The Companies Act, 2013 is drafted on the assumption that human beings are performing these functions. Section relating to vigil mechanism assumes that humans will be filing Protected Disclosure under the vigil mechanism to the heads of the committee[5]. The head of the committee thereafter will exercise his/her discretion and look into the facts of the case and apply principles of natural justice.

1.4 Research Questions

1. How does the current Statute (Companies Act, 2013 and SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015) regulate a vigil mechanism through AI System?
2. What are some of the legal issues faced while implementing an automated system? For example, lack of transparency regarding the functioning of algorithms, liability of the company, admissibility of evidence, and violation of privacy.
3. How can AI-based analysis, algorithms for auditing and algorithms for privacy be used in whistleblowing systems without breaching any duty owed by the directors?
4. What changes in structure, statutes and regulations need to be made in India to create a legally sound, ethically driven and technologically sophisticated automated vigil system?

This paper is divided into seven parts to investigate the above-mentioned questions. After this introduction, the first part is the Legal Framework Governing Vigil Mechanism. This part will cover Section 177 of the Companies Act 2013, SEBI Regulation 22 and practical applications of policies by companies. The second part is Legal Challenges in Corporate Accountability. This section will explore questions regarding algorithmic bias, failure to follow due process, evidence, and privacy in light of the Digital Personal Data Protection Act, 2023.The third part is Integration of Artificial Intelligence in Vigil Mechanism. This section has covered the application of AI tools in the mechanism, constant monitoring and risk rating. The fourth part is Director Duties and Corporate Accountability. This part will cover duties under Section 166, duties of supervision and the need for human intervention.

[5]Satarkar, G. S. (2026). *Regulating artificial intelligence in India: Legal frameworks, governance challenges, and the path toward a dedicated AI law.* https://www.academia.edu/download/132356505/ARTICLE.pdf

© 2026 International Journal of Advanced Legal Research

The fifth part is Findings and Recommendations. This part will suggest changes to the statute, technical requirements and company governance. Finally, the sixth part is the Conclusion. This section will summarise the legal developments in relation to AI driven corporate vigil in India.[6]

2. Legal Framework Governing Vigil Mechanism

2.1 Statutory Foundations under the Companies Act, 2013

The requirement of enacting a Vigil Mechanism by Indian companies is a move towards better corporate governance and was done mainly to avoid major corporate failures that were due to lack of monitoring over the management. The statutory basis of this is given in section 177(9) of the Companies Act, 2013 along with Rule 7 of the Companies (Meetings of Board and its Powers) Rules, 2014.Section 177(9) says that every listed company and certain specified classes of unlisted public and private companies shall have a Vigil Mechanism whereby directors and employees can report genuine concerns as prescribed. The section 177 provides that the Vigil mechanism shall be handled by the Audit Committee of the Board of Directors. This section also states that the Vigil mechanism should ensure that employees and directors are not harassed for using the mechanism (Section 177(10)). In exceptional circumstances, they will have direct access to the Chairperson of the Audit Committee.[7]

[6] Ramya, E. (2026). Whistleblower Protection and Corporate Governance in India: A Critical Analysis of the Effectiveness of the Vigil Mechanism. *International Journal of Legal Science and Innovation, 8*(1), 1-14.https://doi.org/10.63108/IJLSI.7005

[7] Government of India — Companies Act, 2013: MCA Companies Act 2013 Portal

© 2026 International Journal of Advanced Legal Research

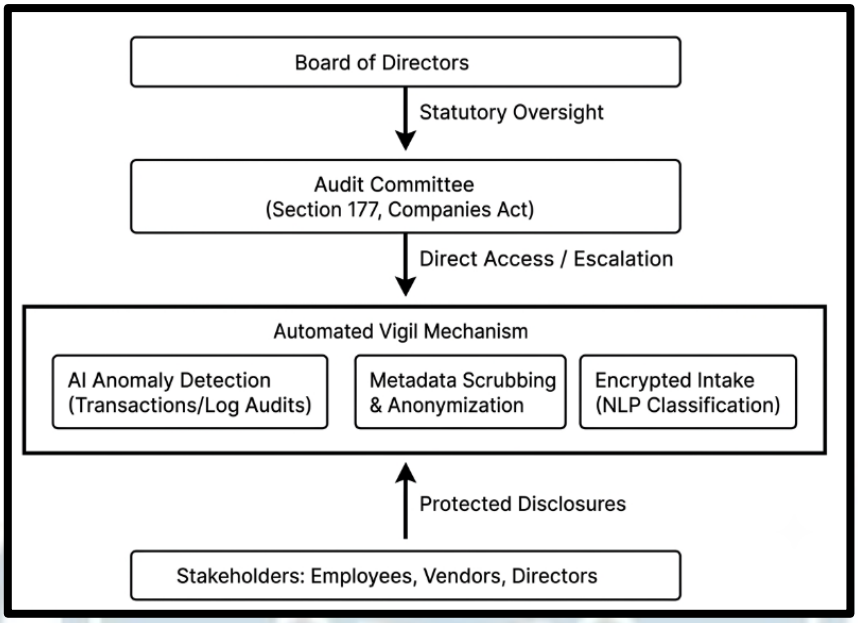


Fig 2.1: Whistleblower Vigil Mechanism and Governance Framework

2.2 Regulatory Architecture under SEBI LODR Regulations

Other than the provisions made under the Companies Act, 2013, there are various regulatory requirements made by the Securities and Exchange Board of India. Regulation 22 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (SEBI LODR) requires that listed companies should have an elaborate Whistleblower Policy. SEBI has made sure that the interests of stakeholders are safeguarded through an expanded definition of the whistleblower. The definition now includes directors, contract laborers, individual consultants, vendors, etc., along with permanent employees.[8]

Further, Regulation 18 of SEBI LODR provides that Regulation 34(3), along with Schedule V requires detailed disclosures concerning the functioning and operation of the 'Vigil Mechanism' in the Annual Corporate Governance Report. Furthermore, listed entities must state that no employees were denied access to the chairman of the Audit Committee and also disclose the total number of complaints of unethical behaviour that they received, investigated and resolved during the financial year. The vigil mechanism has also been expanded under the SEBI (Prohibition of Insider Trading) Regulations, 2015 to cover instances of financial irregularity, market manipulation and the leakage of Unpublished Price

[8] SEBI — LODR Regulations, 2015: SEBI Legal Regulations Portal

© 2026 International Journal of Advanced Legal Research

Sensitive Information (UPSI). Therefore, the vigil mechanism also becomes a market governance mechanism which aims to ensure integrity in the market and therefore uphold the value of shares held by the public.[9]

2.3 Operational Design: Industry Norms and the Mindteck Case Study

The operationalization of legal vigil mandates is clearly illustrated in the corporate governance structures of established technology entities. Mindteck (India) Limited—a publicly traded engineering services and digital transformation firm operating across high-impact verticals including medical devices, data storage, analytical instruments, and semiconductors—provides a definitive corporate case study. In compliance with Section 177 of the Companies Act and Regulation 22 of SEBI LODR, Mindteck maintains a comprehensive Whistleblower Policy that defines the operational boundaries of its vigil mechanism.

The Mindset Vigil Framework encompasses certain key guidelines to report and address any issues that may arise. Issues can be reported by current/previous employees, contract employees, directors, vendors, consultants under Section 177(9) of Companies Act and Regulation 22 of SEBI LODR. The report will be directly submitted to the Chairperson of the Audit Committee via encrypted email/post (Section 177(10) of Companies Act and Regulation 18 of SEBI LODR). Investigations will be completed within 45 days from their disclosure under Internal QMS and ISO guidelines. Whistleblowers are protected against termination, demotion, non-promotion or harassment (Section 177(10) of Companies Act). Any individual making 3 or more false frivolous complaints will get disqualified and will be subjected to disciplinary actions under Rule 7 of Companies Rules. Any individual not satisfied with the decision of the Audit Committee can appeal to the Board of Directors by following the principles of Natural Justice and Corporate Governance Code.

Mindteck has procedures in place for handling disclosures. Protected disclosures must be submitted in writing to the Chairperson of the Audit Committee. The person making the

[9] Agarwal, A. (2018). SEBI (LODR)(Amendment) Regulations, 2018: A route to achieving a global level corporate governance structure in India. *Supremo Amicus*, *7*, 32. https://access.heinonline.com/HOL/Page?handle=hein.journals/supami7&div=8&g_sent=1&casa_token=

© 2026 International Journal of Advanced Legal Research

disclosure will be asked to conceal their identity, and an impartial investigation of the matter will ensue. It is worth noting that the procedure will ensure that the investigation is done within 45 days. It also provides protection from any employment related reprisals and allows the individual to appeal to the full Board of Directors. To prevent the system being abused, individuals are disqualified from the protections offered by the policy if they make frequent frivolous/malicious disclosures (3 or more bad faith reports).[10]

2.4 Legal Assessment: Human Versus Automated Frameworks

Traditional legal requirements can therefore cause issues regarding alignment of processes. The statutory framework assumes that the process is fully manually driven. This means that if a human whistleblower identifies wrongdoing they will produce a report manually, and committee members will also be human and will investigate based on the evidence using natural justice.[11]

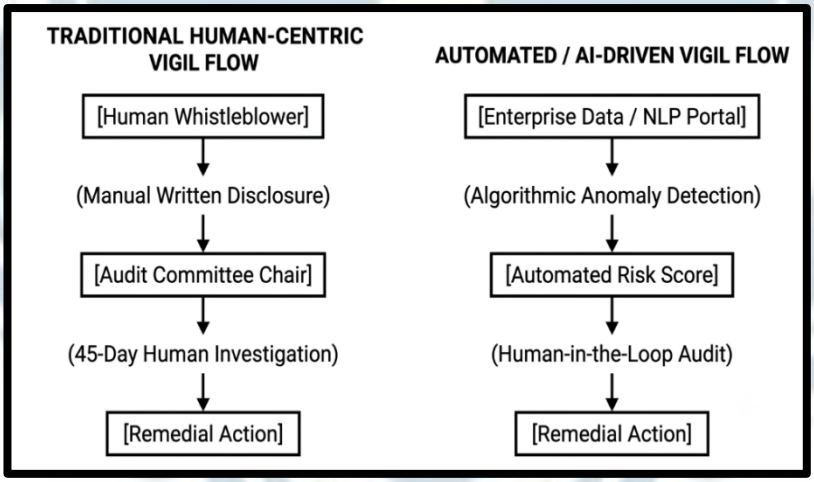


Fig 2.2: Comparative Legal Analysis: Human vs. Automated Frameworks

This is however changed by automated monitoring systems as they have in-built algorithms for processing data, cleaning metadata and providing a risk score. Although these automated systems increase confidentiality and efficiency there are no provisions under Indian law regarding alerts provided by algorithms. It is unclear whether if an AI system detects any

[10]Mindteck (India) Limited (2026/2024): Mindteck Investor Relations & Financial Reports

[11] Farooq, U., Nasir, A., & Khan, K. I. (2026). Towards a 4P framework of financial statement fraud: A systematic literature review. *International Journal of Management Reviews, 28*(2), e70005. https://onlinelibrary.wiley.com/doi/abs/10.1111/ijmr.70005

© 2026 International Journal of Advanced Legal Research

financial manipulation independently it would be considered a Protected Disclosure. There are also issues of natural justice when using automated processes. The Subject (the executive being accused) has a right to view adverse evidence and question witnesses under Indian administrative law. If the main evidence comes from a complex ML model then in order to satisfy natural justice the algorithm should be made clear.

3. Legal Challenges in Corporate Accountability

3.1 Addressing Bias, Discriminatory Results, and Legal Due Process in Algorithms

The use of artificial intelligence in corporate monitoring systems presents a number of legal issues. For example, if an automated risk scoring system was trained using historical disciplinary data it may result in the system associating higher risk with particular departments, regions or employee types due to them being disproportionately disciplined in the past.[12]

This goes against the basic principles of due process and natural justice (audi alteram partem) in Indian administrative and corporate law. If an employee or director suffers any disciplinary action, demotion or reputational impact as a result of any compliance alerts raised by AI systems, they must be given clear explanations as to why they have received this negative outcome. However, many modern Deep Learning models are black box models meaning they produce risk scores using complex non-linear mathematics that cannot be interpreted. This means that if a corporate Board takes action based on an inexplicable AI alert they would be breaching their legal rights to a fair hearing. The organisation would therefore be at risk of legal action regarding unfair dismissal, constructive dismissal and administrative unfairness.

[12]Lognoul, M. (2025). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act–AI Act). *Revue du Droit des Technologies de l'information*, (3-4), 145-189. https://researchportal.unamur.be/en/publications/regulation-eu-20241689-laying-down-harmonised-rules-on-artificial/

© 2026 International Journal of Advanced Legal Research

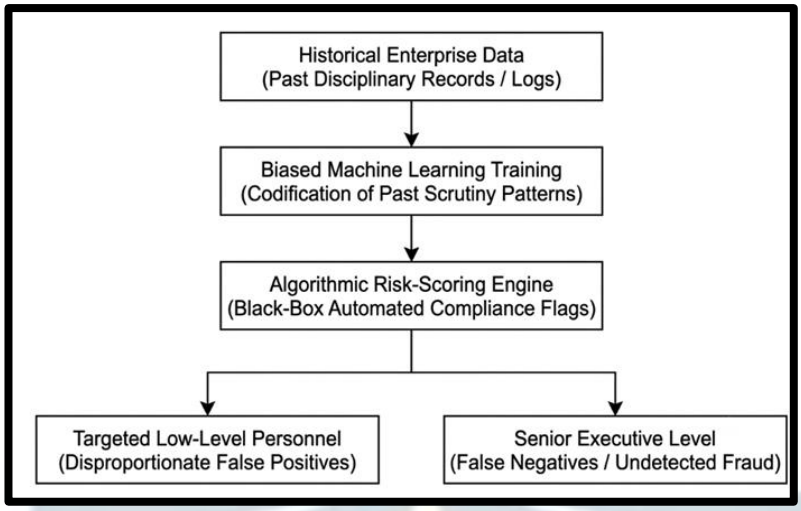


Fig 3.1: Black box AI Flagged Automation

3.2 Evidentiary Admissibility of AI-Generated Data

One significant legal hurdle to enforcing AI driven corporate vigilance lies within the Indian legal system with regards to the admissibility of machine generated outputs. The law on electronic records has been included as Section 63B of Bharatiya Sakshya Adhiniyam, 2023 (BSA), within the Indian legal framework. It replaces Section 65B of the Indian Evidence Act, 1872. In order to present digital records (including AI analysis reports, automated auditing trails and NLP disclosure transcripts), the person presenting the evidence will have to comply with strict statutory requirements. These include providing a certificate under section 63B of the BSA to ensure that the computer system used to create the electronic record was intact, working consistently and unbreached.[13]

In the absence of evidentiary requirements being met under the statutes, the AI generated reports would be inadmissible. This would mean that a corporate board would be unable to provide any legal basis to justify sanctioning under a disciplinary procedure. However, in India, it is widely opposed to extend legal person to algorithms as they do not have any moral agency, financial capital to provide compensation to the courts, nor can they be punished. The Indian legal principles dictate that there needs to be an overseeing body of humans. A corporate board cannot avoid liability under the statutes by using the black box algorithms to monitor as ultimately there is a legal responsibility on humans.

[13] Government of India — Bharatiya Sakshya Adhiniyam, 2023: Press Information Bureau Notice

© 2026 International Journal of Advanced Legal Research

3.3 Privacy Frameworks: DPDPA 2023 Compliance

Table 3.1: Framework based on DPDPA 2023 Compliance[14]

DPDPA 2023 Statutory Principle	Compliance Challenge in Automated Vigil Frameworks	Mandatory Operational Safeguard
Notice and Lawful Consent (Section 6)	There is a conflict between having clear consent for AI monitoring and ensuring investigations remain private and unbiased.	Rely on statutory compliance exemptions pursuant to DPDPA Section 7 or obtain policy consent in the onboarding process.
Purpose Limitation (Section 7)	Data collected by enterprises for normal IT support cannot be used in machine learning monitoring without consent	Implement strict logical data siloing and limit AI training models to explicitly authorized compliance data streams only.
Data Minimization (Section 8)	Often AI tools will collect large amounts of communication data from an enterprise which includes irrelevant personal information about employees	Deploy automated edge-scrubbing algorithms to remove non-relevant personal attributes before ML risk ingestion.
Rights of Data Principals (Sections 11–13)	Whistleblowers and those exercising their right to access or delete information can also cause issues with ongoing sensitive investigations.	Enforce statutory exemptions for legal processes and corporate compliance requests pursuant to the DPDPA framework.

[14] Government of India — Digital Personal Data Protection Act, 2023: Cyber Laws India Official Text Portal

© 2026 International Journal of Advanced Legal Research

These automated surveillance measures must also be compliant with India's principal privacy legislation- Digital Personal Data Protection Act, 2023 (DPDPA). Further, as machine learning models require processing large amounts of data, including that relating to employee communications, system access logs, vendor transactions and personal data, the automated surveillance measures employed would fall within organizations' obligations to employees relating to their data privacy rights and obligations to whistleblowers under legislation.

4. Integration of Artificial Intelligence into Vigil Mechanism

4.1 Technological Architecture of Automated Whistleblowing Systems

The design of a modern automated vigilance system means there is a very complex set up. The system has to be very secure, it has to allow anonymous data collection, provide intelligent analysis and integrate with enterprise systems. An enterprise level automated whistleblower system will integrate directly with ERP, HRIS, electronic data repositories and company communications.[15]

AI determines a risk category (Critical, High, Moderate, Low) and automatically routes the allegation. Critical allegations relating to Senior Management or above and/or of high financial value will automatically be escalated outside the management structure to the Chairperson of the Audit Committee, ensuring we are compliant under section 177 of the Companies Act. Low risk administrative complaints will be passed to the relevant HR team with tracking to ensure there is no delay in processing the issue.[16]

4.2 Comparative Technical Evaluation of Whistleblower Frameworks

To understand the operational impact of AI integration, corporate whistleblowing mechanisms can be categorized into three generational models:

[15] Ramya, E. (2026). Whistleblower Protection and Corporate Governance in India: A Critical Analysis of the Effectiveness of the Vigil Mechanism. *International Journal of Legal Science and Innovation*, *8*(1), 1-14.https://doi.org/10.63108/IJLSI.7005

[16] Bergman, M. M., Bergman, Z., Teschemacher, Y., Arora, B., Jyoti, D., & Sengupta, R. (2019). Corporate responsibility in India: Academic perspectives on the Companies Act 2013. *Sustainability*, *11*(21), 5939. https://www.mdpi.com/2071-1050/11/21/5939

© 2026 International Journal of Advanced Legal Research

Table 4.1: Generation Tiers of Whistleblower Frameworks[17]

Operational Feature	Generation Tiers		
	Traditional Manual Vigil	**Digitized Web Portals**	**Automated AI-Driven Vigil Mechanisms**
Intake Modality	Physical dropboxes, manual mail, unencrypted email	Secure web forms, dedicated third-party hotlines	Multi-lingual NLP portals, secure voice intake, continuous API data feeds
Identity Protection	Policy guarantees against retaliation; manual redaction	Basic technical anonymization (IP address removal)	Algorithmic anonymization, NLP stylometric rewriting, voice pitch shifting
Data Processing & Triage	Manual review by compliance officer or committee secretary	Manual categorization; basic keyword filters	Machine learning predictive risk scoring, automated categorization
Fraud Detection Capability	Reactive only; relies entirely on human disclosure	Reactive; manual attachment review	Proactive and continuous; real-time ERP/HRIS anomaly detection
Audit Committee Interface	Physical reports; periodic quarterly	Digital PDF digests; email notification workflows	Real-time interactive dashboard, immutable audit

[17] Examiners, A. (2024). o. CF (2022). Occupational fraud 2022: A report to the nations. *ACFE Austin, TX*.

© 2026 International Journal of Advanced Legal Research

	presentation		trails, automated SLA tracking
Risk of Human Error / Bias	High risk of subjective screening, leak of identity, or delayed escalation	Moderate risk of manual triage delays or accidental identity exposure	Algorithmic bias potential; requires explainability and human oversight

A key weakness of traditional corporate vigil systems is the risk that records will be altered after intake; files deleted without authorisation or complaints hidden by internal IT administrators or senior executives. If a high level executive is involved in the disclosure then traditional digital databases are at risk of being overridden or logs altered by an administrator. This can be overcome by using an automated system using AI ingestion and audit logs.[18]

Once a Protected Disclosure comes into the system, it is given a cryptographic hash, which forms a digital fingerprint with a timestamp, content payload, and risk rating. The hash is registered on a blockchain, or immutable audit trail that cannot be tampered with by anyone from the company, including the system administrators. Any further actions in the process - notes from the Audit Committee review, assigning of investigators, uploading of evidence and final resolution – get a cryptographic hash and are appended to the case log. The immutable technology will help ensure that all the records will be verifiable for the purposes of SEBI, statutory financial auditors, or judiciary in accordance with Section 63B of the Bharatiya Sakshya Adhiniyam, 2023 and confirm that there were no acts of disclosure concealment or evidence tampering in the company.

5. Director Duties and Corporate Accountability

5.1 Fiduciary Duties under Section 166 of the Companies Act, 2013

[18] Government of India. (2023). Digital Personal Data Protection Act, 2023.

© 2026 International Journal of Advanced Legal Research

The incorporation of automation and technology has not absolved the Board of Directors from their responsibilities. The fiduciary duties of directors in India have been clearly stated under section 166 of the Companies Act, 2013. This was a major change as it moved away from common law principles and instead established a stricter principle for a director under statute.

Sections of this provide obligations of directors to act in a certain manner towards implementing AI compliance technologies[19]:

- Sec. 166(2) Duty to Act in Good Faith and Best Interests: Directors must act in good faith to further the objects of the corporation to confer benefits on members of the corporation as a whole. Directors must also ensure that employees of the corporation, local community and environment are acting in their best interests. By using AI compliance technologies that have not been verified to be accurate, you are breaching this duty by creating bias flags and missing any fraud within the company.
- Sec. 166(3) Due Care and Diligence: The directors should perform their duties with reasonable care. In case the directors do not consider the skills and capabilities of the technological platform on which they are delegating their duties, they will be in breach of their duty of due diligence.
- Sec. 166(4) Duty not to Place Self Interest above that of Corporation: Directors must not cause themselves to be placed in a position where they have a conflict of interest, either directly or indirectly. For example, if the director was to manipulate the criteria used for customising the AI to prevent warnings being issued.

5.2 Governance Oversight: Legal Liabilities of Independent Directors and Audit Committees

The responsibility of establishing an effective vigil mechanism lies with Independent Directors on the Audit Committee. Independent Directors have a responsibility to satisfy themselves under Section 149(8) read with Schedule IV (Code for Independent Directors) of

[19] Nath, P. (2026). Significance Of New Criminal Laws in Today's India–An Analysis. *Journal of Legal Research and Polity*, *3*(1), 19-31. https://jlrp.in/index.php/jlrp/article/view/64

© 2026 International Journal of Advanced Legal Research

the Companies Act, 2013, that adequate control and risk management processes exist within the company and the company has an active and vigorous vigil mechanism.[20]

The Audit Committee can also undertake certain activities under section 177(4), including the review of internal financial controls, risk management systems, and compliance with statutes. In case of a listed entity, if an automated vigil system is deployed by the entity, the members of Audit Committee will not be able to regard the AI tool as a mere software. Due to the nature of false negatives (where material errors that would be detected via a human-based approach are not detected by the automated approach), Independent Directors may incur personal liability under Section 149(12) of the Companies Act, 2006. As per section 149(12), Independent Directors are individually liable for any acts of omission or commission committed by the company if they had knowledge, consented to, connived at or did not act diligently. Therefore, if the Audit Committee does not perform the function of auditing, validating and overseeing the automated vigil system, members of Audit Committee will be subject to regulatory action by SEBI.

5.3 Evaluating the Human-in-the-Loop Paradigm and the Doctrine of Meaningful Human Control

Corporate law requires automated surveillance systems to comply with the 'Human-in-the-Loop' (HITL) requirement meaning they must be subject to Meaningful Human Control (MHC)[21]. This principle stems from administrative law and technology regulation and defines how an autonomous or AI system should not be the final decision maker in situations which will affect legal rights, professional careers and statutory compliance.

Within automated whistleblowing frameworks, Meaningful Human Control requires a structured division of responsibility:

[20]Naphade, N. N. (2021). Company Secretaries as Chief Governance Officers in Indian Companies. *J. on Governance*, *4*, 138. https://access.heinonline.com/HOL/LandingPage?handle=hein.journals/jnlogvane4&div=20&id=&page=

[21] Kaur, H. (2018). Securities market in India: Regulation of undesirable practices by the Securities and Exchange Board of India. In *Regulations and applications of ethics in business practice* (pp. 273-293). Singapore: Springer Singapore. https://link.springer.com/chapter/10.1007/978-981-10-8062-3_15

© 2026 International Journal of Advanced Legal Research

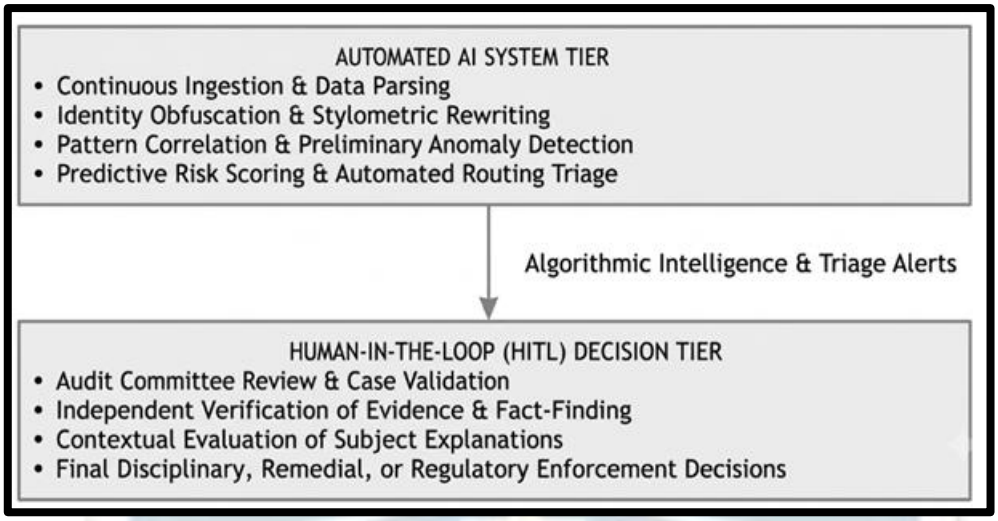


Fig 5.1: Collaboration between AI Tier and HITL Tier

Under a legally compliant HITL[22][23]model:

a. AI as a Tool of Analysis: The automated vigil tool serves as an analysis engine. Software performs data analysis, removes identifying information from disclosures, detects transaction anomalies, and discovers any policy violation.
b. Human Exclusivity in Determining Outcomes: The automated vigil tool cannot decide whether there is no Protected Disclosure; impose sanctions on the worker who has made such a disclosure; or close the inquiry. All determination is in the hands of humans alone and that too of Compliance Officers and Audit Committee.
c. Circumventing Automated Evaluations: Human bodies need to have the ability to circumvent assessments made by the automated AI engine. For example, in case the engine evaluates complex disclosure with a low risk score because of new language or the absence of training parameters, human compliance professionals need the ability to elevate it to a full investigation.

[22] Oelrich, S., & Erlebach, K. (2021). Taking it outside: A study of legal contexts and external whistleblowing in China and India: Oelrich S., Erlebach K. *Asian Journal of Business Ethics*, *10*(1), 129-151. https://link.springer.com/article/10.1007/s13520-021-00125-y

[23] Farooq, U., Nasir, A., & Khan, K. I. (2026). Towards a 4P framework of financial statement fraud: A systematic literature review. *International Journal of Management Reviews*, *28*(2), e70005. https://onlinelibrary.wiley.com/doi/abs/10.1111/ijmr.70005

© 2026 International Journal of Advanced Legal Research

d. Implementation of Meaningful Human Control would ensure that technology enhances the scope of auditing without substituting the human element and ensuring legal control through the Board of Directors.

5.4 Governance Case Study: The Mindteck Board Model

The practical balance between board, committees and technology can be seen in the corporate governance structure of Mindteck (India) Limited[24]. The company has a clear division of roles between the executive management and independent directors. The company has an appropriately structured Board of Directors with Non-Executive and Independent Directors. The directors have expertise in Information Technology, Finance, Legal, Corporate Governance and Global Business.

6. Findings and Recommendations

6.1 Summary of Core Empirical and Legal Findings

There are several implications for the implementation of automated vigil mechanisms under Indian Corporate Law[25]:

a) There are currently insufficient statutory provisions relating to automated vigil mechanisms in Indian Corporate Law. The current provisions under Section 177 of the Companies Act 2013 and SEBI LODR Regulation 22 assume that vigils will be manually conducted. As such there is no statutory definition of what constitutes algorithmic alerts, automated auditing or NLP disclosures.

b) There is increased risk of algorithmic bias, opaque risk assessment and lack of procedural fairness in relation to ML. In case organizations lack measures to stop the black-box approach, there may be problems in the way that automated vigil systems are applied.

c) There are stringent conditions for the admission of AI audit reports and automated interactions records as per the Bharatiya SakshyaAdhiniyam 2023 (Section

[24]Mindteck (India) Limited (2026/2024): Mindteck Investor Relations & Financial Reports
[25] Saha, P., Yu, Y., & Wang, Y. (2026): arXiv Paper 2610.08554

© 2026 International Journal of Advanced Legal Research

63B).These require audit trails to be able to be verified, hash values and verification of the system.

d) There is a thin line between statutory duties to the whistleblowers and employee privacy under the Digital Personal Data Protection Act 2023. If companies are continually monitoring using AI they may face issues with data minimisation unless they have automated anonymisation at the edge and logical segregation.

Statutory duties cannot be delegated to automated systems. Section 166 and 149(12) of the Companies Act means that companies have a duty to ensure they are integrity. This must therefore be ensured by directors and Audit Committee members. They must maintain Meaningful Human Control and use AI as a tool to help with analysis.

6.2 Proposed Statutory Amendments to the Companies Act and SEBI LODR

For dealing with the issues of law, statutory regimes in India need to evolve so that they support the automated surveillance system[26]:

6.2.1 Amendments to Section 177, Companies Act, 2013

Section 177(9) should have an additional clause that would acknowledge automation of vigil functions:

"Provided that where a company establishes an automated or artificial intelligence-driven vigil mechanism, any objective risk alert or anomaly report generated by such system concerning material financial irregularity, fraud, or statutory non-compliance shall be deemed to be a Protected Disclosure, requiring mandatory triage and review by the Audit Committee."

6.2.2 Amendments to SEBI LODR Regulations

Regulation 22 of SEBI needs to be amended such that any listed company using AI compliance systems should have a formal technology governance framework[27]:

[26] SEBI — LODR Regulations, 2015: SEBI Legal Regulations Portal
[27] Satarkar (Nale), G. S. (2026): WISDOM Journal Paper Entry

© 2026 International Journal of Advanced Legal Research

- Mandatory Algorithmic Audits: Any listed company which uses machine learning compliance systems should have mandatory algorithmic audits done each year by an external auditor, and should produce a certificate along with their corporate governance report.
- Threshold for Escalation: The regulations need to define threshold parameters where the high risk needs to be automatically escalated to the Chairman of the Audit Committee.

6.2.3 Harmonization under DPDPA 2023

It is incumbent upon The Ministry of Electronics and Information Technology (MeitY) to make specific rules regarding DPDPA that the processing of metadata of communications of employees for statutory vigil purposes falls within the definition of "Legitimate Uses" specified in Section 7 if the organization employs automation techniques for anonymizing data.[28]

6.3 Comparative International Frameworks and Lessons for India

When considering the long-term legal strategy for governing AI in corporations, India can learn much from international comparative models:

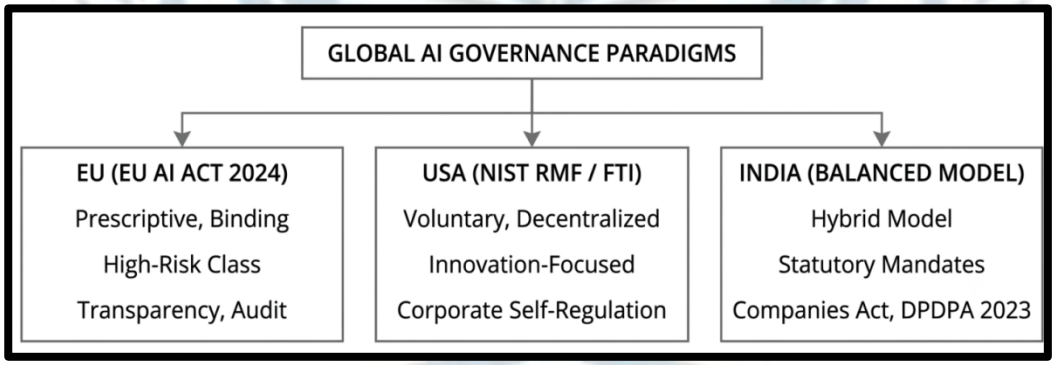


Fig 6.1: Global AI Governance Paradigms

6.3.1 The European Union Model (EU AI Act, 2024)

According to the AI Act of the European Union, there is a risk-based prescriptive and legally-binding framework. The EU AI law classifies AI technologies that have been used for

[28] Government of India — Digital Personal Data Protection Act, 2023: Cyber Laws India Official Text Portal

© 2026 International Journal of Advanced Legal Research

employee surveillance, hiring processes, credit scoring, and risk assessment as "High-Risk AI Systems." High-risk AI systems are subject to many legal requirements, such as mandatory conformity assessment and continuous risk management documentation. In case the risk-based classification model is adopted by India, automation-based vigilance tools for monitoring transactions as well as communications at the company level would become high-risk compliance tools that require auditing as well as an explanation.[29]

6.3.2 The United States Model (NIST AI RMF & Executive Frameworks)

On the other hand, the U.S. takes a decentralized and sector-focused policy model, which is informed by voluntary models such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework. U.S. approach puts a lot of weight on technological innovation, which is accomplished using self-regulation of corporations, along with regulation from bodies like FTC.[30]

6.4 The Hybrid Pathway for India

India is perfectly positioned to adopt a dual regulation framework that balances the structural features of the EU model and the flexibility of the US model. India will be able to ensure the use of technology in corporate governance through the establishment of risk categories for AI technologies in corporate law.[31]

7. Conclusion

7.1 Synthesis of the Argument

The transition from manual whistleblowing systems to automated AI-based vigil systems is a significant development in corporate governance. Modern organizations need automation in

[29] European Parliament & Council — EU AI Act, 2024: EUR-Lex Regulation (EU) 2024/1689

[30] Agarwal, A. (2018). SEBI (LODR)(Amendment) Regulations, 2018: A route to achieving a global level corporate governance structure in India. Supremo Amicus, 7, 32. https://access.heinonline.com/HOL/Page?handle=hein.journals/supami7&div=8&g_sent=1&casa_token=

[31] Lognoul, M. (2025). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act–AI Act). Revue du Droit des Technologies de l'information, (3-4), 145-189. https://researchportal.unamur.be/en/publications/regulation-eu-20241689-laying-down-harmonised-rules-on-artificial/

© 2026 International Journal of Advanced Legal Research

order to have continuous monitoring and quick information processing. This can be done through automation by using vigilant systems through the application of natural language processing for anonymization of identities, machine learning for transaction auditing and risk scoring for prioritization of complaints. But the problem is that technology needs to be legally compatible. This paper will show how incorporating AI into a corporate vigil system causes multiple legal implications under Indian corporate law.

Provisions such as Section 177 of the Companies Act, 2013 and SEBI LODR Regulation 22 were formulated based on some assumptions related to compliance. Automated processes will pose problems as they are likely to have issues relating to algorithmic bias, issues relating to admissibility of evidence under Section 63B of the Bharatiya Sakshya Adhiniyam, 2023, issues relating to data privacy under the Digital Personal Data Protection Act, 2023 and procedural breaches.[32]

It is important to note that the Indian corporate law jurisprudence provides that statutory fiduciary obligations cannot be delegated to the software algorithms. As per Section 166 and Section 149(12) of the Companies Act, the directors and members of the Audit Committee have non-delegable obligations to maintain integrity in the corporate world. Thus, procedures of vigilance using automation should be in line with the Meaningful Human Control principle.

7.2 The Future Horizon of Corporate Governance and Technology

With advancements in the field of artificial intelligence, the future of corporate governance is expected to involve automated compliance technologies. With the advent of new technological paradigms, such as generative AI assistants, cryptographically secure ledgers, and automated continuous audit pipelines, corporate organizations would be transformed in terms of their processing of ethical disclosures, monitoring of financial health, and management of risks.

In the context of the Indian corporate world, the effective implementation of technological evolution would involve alignment of the corporate practice with statutory and judicial

[32] Farooq, U., Nasir, A., & Khan, K. I. (2026). Towards a 4P framework of financial statement fraud: A systematic literature review. International Journal of Management Reviews, 28(2), e70005. https://onlinelibrary.wiley.com/doi/abs/10.1111/ijmr.70005

© 2026 International Journal of Advanced Legal Research

interpretations. Technology companies like Mindteck (India) Limited, which is publicly listed, serve as an example of how technological development and compliance governance can be aligned for creating organizational resilience[33]. The Indian corporate vigil framework can be created through enactment of relevant statutory amendments, auditing standards, and Human-in-the-Loop protocols. In summary, automated whistle-blowing systems ought not to be perceived in a wholly optimistic light as fail-proof compliance solutions or be dismissed out of fear for their opacity.

References

Agarwal, A. (2018). SEBI (LODR)(Amendment) Regulations, 2018: A route to achieving a global level corporate governance structure in India. *Supremo Amicus*, *7*, 32.https://access.heinonline.com/HOL/Page?handle=hein.journals/supami7&div=8&g_sent=1&casa_token=

Bergman, M. M., Bergman, Z., Teschemacher, Y., Arora, B., Jyoti, D., & Sengupta, R. (2019). Corporate responsibility in India: Academic perspectives on the Companies Act 2013. *Sustainability*, *11*(21), 5939.https://www.mdpi.com/2071-1050/11/21/5939

Examiners, A. (2024). o. CF (2022). Occupational fraud 2022: A report to the nations. *ACFE Austin, TX*.

Farooq, U., Nasir, A., & Khan, K. I. (2026). Towards a 4P framework of financial statement fraud: A systematic literature review. *International Journal of Management Reviews*, *28*(2), e70005.https://onlinelibrary.wiley.com/doi/abs/10.1111/ijmr.70005

Government of India. (2023). Digital Personal Data Protection Act, 2023.

Kaur, H. (2018). Securities market in India: Regulation of undesirable practices by the Securities and Exchange Board of India. In *Regulations and applications of ethics in business practice* (pp. 273-293). Singapore: Springer Singapore.https://link.springer.com/chapter/10.1007/978-981-10-8062-3_15

Lognoul, M. (2025). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act–AI Act). *Revue du Droit des Technologies de*

[33]Mindteck (India) Limited (2026/2024): Mindteck Investor Relations & Financial Reports

© 2026 International Journal of Advanced Legal Research

l'information, (3-4), 145-189.https://researchportal.unamur.be/en/publications/regulation-eu-20241689-laying-down-harmonised-rules-on-artificial/

Naphade, N. N. (2021). Company Secretaries as Chief Governance Officers in Indian Companies. *J. on Governance*, *4*, 138.https://access.heinonline.com/HOL/LandingPage?handle=hein.journals/jnlogvane4&div=20&id=&page=

Nath, P. (2026). Significance Of New Criminal Laws in Today's India–An Analysis. *Journal of Legal Research and Polity*, *3*(1), 19-31.https://jlrp.in/index.php/jlrp/article/view/64

Oelrich, S., & Erlebach, K. (2021). Taking it outside: A study of legal contexts and external whistleblowing in China and India: Oelrich S., Erlebach K. *Asian Journal of Business Ethics*, *10*(1), 129-151.https://link.springer.com/article/10.1007/s13520-021-00125-y

Ramya, E. (2026). Whistleblower Protection and Corporate Governance in India: A Critical Analysis of the Effectiveness of the Vigil Mechanism. *International Journal of Legal Science and Innovation*, *8*(1), 1-14.https://doi.org/10.63108/IJLSI.7005

Satarkar, G. S. (2026). *Regulating artificial intelligence in India: Legal frameworks, governance challenges, and the path toward a dedicated AI law*.https://www.academia.edu/download/132356505/ARTICLE.pdf

European Parliament & Council — EU AI Act, 2024: EUR-Lex Regulation (EU) 2024/1689

Government of India — Bharatiya Sakshya Adhiniyam, 2023: Press Information Bureau Notice

Government of India — Companies Act, 2013: MCA Companies Act 2013 Portal

Government of India — Digital Personal Data Protection Act, 2023: Cyber Laws India Official Text Portal

Mindteck (India) Limited (2026/2024): Mindteck Investor Relations & Financial Reports

Saha, P., Yu, Y., & Wang, Y. (2026): arXiv Paper 2610.08554

Satarkar (Nale), G. S. (2026): WISDOM Journal Paper Entry

SEBI — LODR Regulations, 2015: SEBI Legal Regulations Portal

© 2026 International Journal of Advanced Legal Research