JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Whistleblowing in the Digital Age: AI-Based Fraud Detection and Corporate Ethics in India

CS Vihasi Shah, Dr. Namrata Luhar

PhD Research Scholar, The Maharaja Sayajirao University of Baroda, vihasishah@gmail.com

Associate Professor of Law, The Maharaja Sayajirao University of Baroda, luhar.namrata-law@msubaroda.ac.in

ABSTRACT *:* Whistleblowing is an important tool in corporate governance that uncovers unethical and fraudulent actions within organizations. In the wave of the digital world, artificial intelligence (AI) is a game-changing innovation behind people on their whistleblowing journey in fraud detection. This research investigates the nexus between AI-based fraud detection technology and corporate ethics in India and how technological innovations could bolster corporate governance. The study starts by defining the concepts of whistleblowing that integrate the ethical basis and legal basis in India. The research paper then discusses AI-based fraud detection systems, including machine learning, predictive analytics, and natural language processing, analyzing their usefulness and potential in detecting financial irregularities and corporate misconduct. Nonetheless, the use of AI for whistleblowing comes with substantial drawbacks, including privacy issues around data, biases built into algorithms, and ethical challenges posed by machine-based decision-making. This study critically assesses these issues and finds gaps in the Indian legal framework relating to an AI-integrated whistleblowing system. This research paper highlights the importance of balancing the efficiency of AI with ethical imperatives in the design and implementation of whistleblower systems and also discusses how AI-driven whistleblowers can improve corporate governance in India, which contributes to sustainable development.

Key Words*:* Whistleblowing, Corporate Governance, Artificial Intelligence (AI), Fraud Detection, Regulatory Framework

I. Conceptual Framework: Whistleblowing and Corporate Ethics

Whistleblowing basically means to report unethical or illegal practices works as a mechanism of control that helps to detect unethical acts at an early stage, which saves the organization from incurring financial and reputational losses. Historically, whistleblowing depended on humans coming forward using internal organizational reporting systems or regulatory authorities. Nevertheless, these mechanisms were frequently stymied by intimidation, a failure of anonymity, and institutional push-back that discouraged reporting of malpractice.

Whistleblowers play an important role in corporate governance by promoting transparency, accountability, and ethical behavior within the organization. This means reporting wrongdoing, fraud, corruption, or unethical conduct by persons with direct or indirect knowledge of such activities within the organization. Whistleblowers are vital in bringing to light corporate misconduct that otherwise would go unnoticed and stop a trail of financial deception, compliance violation, or reputation damage. Whistleblowing is an internal control mechanism that allows organizations to identify bad behavior and address it before it rears it worsen and turns into a legal or financial nightmare.

Fundamentally, whistleblowing itself carries high ethical implications whose roots lie in the ideals of integrity, justice, and accountability. One can take the deontological perspective and argue that to fulfill morality one must report unethical acts, as it is a more complex obligation that transcends personal morality and presents a general obligation to the corporate world of being more fair and just and upholding ethos. This involves preventing harm to stakeholders and ultimately to the public, including investors, employees, consumers, and society as a whole. To that end, corporate ethics frameworks encourage the whistleblower system to

be protected, to ensure fear of retaliation does not impede reporting misconduct. It strengthens corporate governance structures by promoting an environment of trust and compliance through organizations that support ethical whistleblowing mechanisms.

The most substantial law guiding whistleblowing in India is the Whistle Blowers Protection Act, 2014, which offers a legal framework for disclosing information about corruption or wilful abuse of power within publicly owned organizations. Till date, this is a significant limitation as the law does not include private sector whistleblowers and is limited in its applicability to corruption allegations. In the corporate sector, corporate regulators and stock exchanges have included whistleblower protections in the SEBI Regulations requiring listed companies to formulate and disclose a whistleblower policy, and the Companies Act, 2013 which imposes a duty on certain corporations to establish a vigil mechanism enabling employees and directors to report misconduct. Even with these protections in place, the lack of meaningful protections for whistleblowers working in private corporations indicates that more Legislative reform is necessary.

II. The Role of AI in Whistleblowing and Fraud Detection

The rise of artificial intelligence (AI) in corporate governance has revolutionized whistle-blowing mechanisms and fraud detection. By harnessing computational intelligence, AI-guided systems can help detect anomalies in corporate activities, improve whistleblower defenses, and reduce financial and ethical risks. This development has greatly enhanced the ability of fraud detection, enabling organizations to identify and respond to dishonest practices before they lead to legal breaches. AI-based whistleblowing and fraud detection mechanisms are not only more efficient, accurate, and secure, but also are one of the important steps in modern corporate governance.(Institute of Company Secretaries of India, 2023)

Artificial intelligence-based fraud detection systems use advanced technologies like Machine Learning (ML), Predictive Analytics, Natural Language Processing NLP, etc., to identify and analyze fraud in corporate transactions.

ML algorithms allow analyzing massive amounts of structured and unstructured data to make out patterns linked to fraudulent behavior. These algorithms can identify deviations from common transaction patterns by studying historical data, thus allowing an organization to identify suspicious activity as it happens. Supervised learning algorithms use labeled data sets of known fraud cases to identify similar cases, while unsupervised learning algorithms detect new patterns of fraud that have not been identified before by signaling anomalies in the data set. (Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates, 2024)
Predictive Analytics uses statistical models and data mining techniques to identify the odds of fraudulent activities before they occur. Predictive models can analyze historical fraud data to identify trends and predict behavioral patterns, which can then serve as early alerts to a compliance team for further action. They enable organizations to alert themselves to such "red flags" of potential financial and regulatory misconduct promptly, so that preventive action can be taken.(SQream, 2024)
(NLP) AI systems can analyze textual data including emails, reports, and whistleblower complaints using NLP to identify anomalies that could indicate fraud and misconduct. AI algorithms can analyze lexicon use, sentiment transitions, and less apparent trends in corporate correspondence and detect the warning signs of misconduct ahead of time. NLP can be especially beneficial in evaluating whistleblower submissions, streamlining case reviews, and flagging high-risk complaints for further investigation.(IBM, 2024)

Machine learning uses data to detect intricate patterns in volumes of financial transactions, employee communications and audit reports to mine subtle indicators of misconduct that may evade human auditors. AI recognizes and adapts to changing patterns over time through deep learning, allowing it to identify evolving fraud schemes and offer even more accurate insights. To improve risk assessment, compliance decision intelligence uses predictive analysis to assess each corporate fraud case and develop probability scores for expected corporate activity, allowing compliance teams to prioritize investigations based on risk levels. This allows organizations to mitigate vulnerabilities before they become widespread issues. NLP further enhances the ability of AI to process unstructured data, emails, reports, or whistleblower submissions, for example, is analyzed for general linguistic patterns and sentiments that may reflect fraud or misconduct. NLP systems can be used to automate the classification of reports, assess their credibility, and flag inconsistencies in communications. Moreover, data-based detection models based on ML continuously analyze all financial transactions and employee activity, are capable of finding deviations from normal by adopting behavior models, such as abuse of power for unauthorized money transfer or generation of suspicious purchase orders for company goods. In whistleblower protection, AI-based platforms leverage encryption and anonymization methods to protect whistleblowers' identities and increase the confidentiality of whistleblowing reports. The process is automated, resulting in a faster, more impartial investigation that reduces human factor biases and gives trust to whistle-blowers. The trio of ML, predictive analysis, and NLP, when weaved into corporate governance, can help stiffen the compliance framework, bolster fraud detection, and promote a culture of transparency and accountability.

2.1 Case Studies of AI-Powered Fraud Detection

Case Study 1: AI-Driven Compliance at Infosys, India

In India, Infosys, the country's second-largest IT company, has already turned to AI-powered whistleblowing and fraud detection systems to comb through employee communications and identify signs of corporate wrongdoing. The AI system leverages natural language processing (NLP) to scrutinize emails, chat logs, and internal documents for indications of fraudulent behavior, the potential for conflicts of interest, and insider trading. The AI-powered compliance framework at Infosys is helping bring in the transparency necessary to ensure that whistleblower complaints are processed in a timely and orderly manner.

Case Study 2: SEC — Artificial Intelligence in Whistleblower Protection, United States

The United States Securities and Exchange Commission (SEC) uses AI and ML technologies to process whistleblower reports, as well as to monitor fraud among publicly traded companies. Leveraging AI-driven analytics, the SEC is able to identify cases of high risk, enabling regulators to prioritize investigations and act quickly against corporate misconduct. AI and the SEC Whistleblower Program Recognizing the potential for AI to transform whistleblower protection, the SEC launched a program that incorporates AI with the goal of enhancing the detection of fraud, which has led to an increase in enforcement actions and significant financial recoveries. (Infosys BPM, n.d.)

With the increasing adoption of AI in the corporate governance system of India, the emergence of strong legal endorsement combined with the incorporation of global best practices will be crucial for leveraging the effectiveness of AI-powered whistleblower and fraud detection systems.(Zuckerman & Stock, 2025)

III. Regulatory and Legal Perspectives on AI-Based Whistleblowing in India

The current laws protect whistleblowers and guide corporate behavior, they do not specifically cater to systems of AI-driven whistleblowing. The growing dependence on AI-based solutions for fraud detection and risk mitigation calls for a comprehensive examination of the existing framework of whistleblower protection laws in India, as well as mechanisms to regulate AI governance and legal gaps that may arise, following the introduction of automated whistleblowing systems. The most applicable legislation related to the issue in India is Whistle Blowers Protection Act, 2014, which provides for the protection of whistle-blowers; people who expose wrongdoings, corruption, financial irregularities, or criminal offenses within public service. But it lacks best practices for AI use in the creation of whistleblower reports so important issues concerning algorithmic bias, algorithmic decision-making, and AI-generated whistleblower complaints go unregulated by the Act. Moreover, AI-based reporting systems lack specific provisions that guarantee data confidentiality and privacy, which could lead to the use of sensitive whistleblower data.(Steward, n.d.) For example, under the Companies Act, 2013, a few companies in the corporate sector are obligated to set up a whistleblower protection mechanism by imposing a vigil mechanism under Section 177. (Mondaq, n.d.) Likewise, the Securities and Exchange Board of India (SEBI) Listing Obligations and Disclosure Requirements Regulations, 2015, provide for corporate whistleblower mechanisms. Yet neither of these legal instruments refers explicitly to the use of AI-based fraud detection or whistleblowing systems. Several regulatory provisions covering whistleblowing via AI are not in place, and without proper regulations for whistleblowing, there are vital concerns about how data is used and privacy maintained, the accuracy of AI-generated reports, proper management of AI models, accountability for identifying misconduct, etc. Without comprehensive AI governance frameworks, businesses utilizing AI to identify fraudulent behavior may encounter moral and legal dilemmas around the transparency and fairness of automated whistleblower systems. (Government of India, 2013)

The Digital Personal Data Protection Act, 2023 (DPDP Act), regulating the processing of personal data in India, is important for AI-driven whistleblowing mechanisms, as these systems typically require the large-scale collection and analysis of employee and corporate data. Although the DPDP Act sets out general privacy protections, there are no provisions concerning AI-based decision-making in whistleblowing. Whistleblowers identified through AI systems may also have limited legal means to challenge retaliation, made worse by acting on inaccurate reports generated by AI systems. These developments underscore the urgent need for legislatures and courts to consider how targeted legal interventions can help ensure that AI-driven whistleblower mechanisms comply with data protection standards without undermining protections for whistleblowers. (Securities and Exchange Board of India, 2015)

IV. Strengthening AI-Enabled Whistleblowing in India: Challenges, Ethical Concerns, and Future Prospects

AI-Based Whistleblowing and Fraud detection pose several challenges and ethical concerns that need to be addressed if AI-driven whistleblowing systems are going to be effective, fair, and reliable. The key concerns are related to data privacy and confidentiality, biases in AI algorithms, ethical concerns relating to automated decision-making, and the existing legal gaps in India's regulatory structure. Overcoming these challenges is crucial for the effectiveness of AI-enhanced whistleblowing systems while also protecting the integrity and trustworthiness of the system within the corporate environment.

Data privacy and confidentiality protection is also warned areas for AI whistleblowing. Whistleblower reports often involve sensitive information relating to corporate misconduct, financial/fundamental discrepancies, and unethical practices in business processes. AI systems analyzing such data must strictly adhere to data protection laws to protect the identity of whistleblowers and prevent unauthorized access to confidential information. (Government of India, 2013) India has also enacted the Whistleblowers Protection Act, 2014, which provides a legal framework for protecting whistleblowers in public sector organizations, however, the Act does not enumerate specific provisions regarding data security in AI-driven whistleblowing systems. (European Data Protection Supervisor, n.d.)

Without adequate encryption, secure data storage, and strict access controls, AI-driven whistleblowing platforms risk exposing the identities of whistleblowers, making people reluctant to report misconduct for fear of retaliation.(Ministry of Personnel, Public Grievances & Pensions, 2024)

Moreover, the use of AI-powered whistleblowing platforms might involve the collection, analysis, and storage of vast amounts of information, which could lead to potential data breaches or unauthorized surveillance. If such reports are mishandled or leaked, the integrity of the reporting mechanism as a whole may be compromised, thereby dissuading future disclosures. To prevent privacy risks posed by AI-based whistleblowing, organizations need to engage in solid data governance and comply with international data protection standards like the General Data Protection Regulation (GDPR). (Burman, 2023)

AI technologies are trained on historical data and machine learning algorithms that detect fraud and unethical behavior, however, they can be subject to biases that reach incorrect conclusions. AI algorithmic bias can occur in two main forms: False Positives (Improperly Identifying Fraud Behavior): Due to biases in the training data, AI models may incorrectly classify legitimate business transactions or employee actions as fraudulent. This can lead to unnecessary probes, reputational harm, and false charges of employees or corporate bodies. [17] False Negatives (Missing Real Fraud): On the flip side, there are biased AI models that may miss actual fraud as they fail to identify pseudoscientific explanations regarding corporate misconduct. This can happen if these AI systems are trained on incomplete datasets, or if the fraudsters fiddle around with their behavior to escape detection by these AI algorithms.[18]

AI-driven whistleblowing systems are prone to bias due to biased training data, flaws in algorithm design, and a lack of transparency in decision-making processes. As a case in point, in an AI system trained on data suggesting that fraud is disproportionately prevalent in certain industries, demographic groups, or regions, an unfairly large percentage of applicants from these "at-risk" groups may be incorrectly targeted, and applicants from non-risk groups may escape detection.

It is vital to achieving fairness and minimizing algorithmic bias in AI-based whistleblowing tools models must be audited periodically and it may be further enhanced by using explainable AI (XAI) techniques in fraud detection systems. Data disparities can be reduced by using bias-mitigation strategies, which can potentially leverage diverse and representative training datasets, hence improving the reliability of the ML models. These can be made mandatory by the regulatory bodies to review the AI algorithms used in the whistle-blowing, to ensure that the AI is not biased or questionable. (Anura.io, n.d.)

AI-driven systems have the ability to analyze large volumes of data efficiently, identify anomalies, and mark possible fraud cases. But we cannot leave decisions about disciplinary actions, legal actions, or corporate penalties to the mercy of AI without the control of human input.

Ethical Issues in Automated Decision-Making:

AI-powered whistleblowing systems offer significant advantages in detecting corporate misconduct and financial fraud; however, they also present inherent limitations. One of the primary concerns is the lack of contextual understanding of AI algorithms. While AI can efficiently detect anomalies in financial transactions or employee behavior, it often fails to account for contextual factors such as market fluctuations, operational constraints, or human errors that do not necessarily indicate wrongdoing. This limitation increases the risk of unfounded allegations or disciplinary actions against employees when AI-driven whistleblowing tools operate without human oversight. Another critical issue is the risk of over-surveillance. AI-powered fraud detection and whistleblowing systems often involve continuous monitoring of employee communications, transactions, and workplace activities, potentially leading to concerns regarding employee privacy and ethical considerations. Overreliance on AI for surveillance may foster a culture of mistrust within organizations, thereby discouraging transparency rather than promoting it. Additionally, AI lacks human discretion, which is crucial in assessing whistleblower reports. Effective whistleblowing mechanisms require nuanced judgment, where legal, ethical, and situational factors must be carefully considered. AI, despite its efficiency, lacks the empathy and ethical reasoning necessary to handle whistleblower complaints effectively. To mitigate these risks, organizations can implement a human-in-the-loop (HITL) approach, wherein AI-powered whistleblowing systems function as decision-support tools rather than autonomous decision-makers. This approach ensures that AI does not make independent determinations but instead aids human

oversight in assessing misconduct claims, thereby preserving the integrity of whistleblower protection mechanisms while leveraging AI's analytical capabilities.(Planet Compliance, n.d.)

AI technology is being increasingly adopted in corporate governance and this has greatly improved the efficiency and accuracy of fraud detection mechanisms. In India, AI-based whistleblowing systems can play an important role in spotting financial irregularities, identifying corporate fraud, and leading to a higher level of transparency in organizations. Such a wholesome approach will enable us to maximize the benefits of AI in whistleblowing as well as tackling its inherent risks by improving the abilities of AI, providing ethical frameworks for the use of AI, and augmenting regulatory enforcement. AI-enabled whistleblowing in India will need to work on technological aspects, compliance with ethical parameters, and a legal framework, which would help in leaps and bounds in nurturing a culture of whistleblowing.

AI-powered technology for fraud detection can help reform corporate whistleblowing systems in India. By combining machine learning (ML), predictive analytics, and natural language processing (NLP), can potentially enhance the detection of financial discrepancies and other elements signifying fraudulent behavior. AI-driven models are capable of processing enormous amounts of financial data, audit reports, and employee communications to identify discrepancies that might otherwise remain undetected. Deep learning algorithms strengthen whistleblowing systems by detecting complicated fraud networks and discovering unseen connections in financial activities. With more businesses moving online in India, AI-driven fraud detection solutions need to become a part of the corporate governance framework, enhancing internal controls to curb financial impropriety.

Although AI can greatly help combat fraud and identify whistleblowers, ethical standards have to be in place for its use to be fair, transparent, and accountable. The overarching concern in AI-backed whistleblowing is algorithmic bias, lowering the chances of the goals of detecting fraud reaching full potential via the generation of false positives or negatives. To combat this organizations need to train their AI models and then test them for fairness and accuracy on a continual basis. By using explainable AI (XAI) techniques, we can introduce transparency into the decision-making of systems producing AI-generated whistleblower reports, thereby enabling human auditors of these reports to interpret and validate the reports. Also, solutions for AI-augmented whistleblowing should adopt privacy safeguards, working to protect the identity and privacy of whistleblowers. In this process, it is essential for strong encryption protocols and secure data handling measures to be incorporated to notably prevent unauthorized access to whistleblower reports and protect individuals from potential retaliatory actions.

Meaningful use of AI in whistleblowing also promotes a proper balance between automation and human input. However, final decisions regarding whistleblower reports must involve human involvement as AI may flag a greater number of records than a human may be able to process. Preventing over-reliance on automated decision-making using AI. However, by having AI-generated alerts scrutinized by compliance officers or independent regulatory bodies, individual accountability can still remain through AI-assisted whistleblowing frameworks that facilitate system monitoring. There would also be AI models that can process the data and highlight extraordinary points in the whistleblower complaint and, if needed, make contextual suggestions that can help in addressing the more regimented issues of bias.

The Indian regulatory framework needs to adapt to facilitate AI-enabled whistleblowing systems and define standards for responsible use. Regulatory bodies, like the Securities and Exchange Board of India (SEBI), the Reserve Bank of India (RBI), and the Ministry of Corporate Affairs (MCA), are key in establishing AI governance policies that safeguard whistleblowers while encouraging corporate accountability. As the principal regulator for publicly traded companies, SEBI should mandate transparency requirements for AI, so corporations voluntarily disclose how they process data and how they mitigate bias in their datasets when deploying AI-driven whistle-blowing systems. As the apex authority to oversee banking and financial institutions, RBI should come up with AI governance norms to prevent AI-driven financial misappropriation and strengthen the fraud detection mechanisms in the financial sector. Finally, the Ministry of Corporate Affairs should take a lead role in developing AI-specific provisions in India's corporate governance structure, and in creating a standard for AI-friendly whistleblowing mechanisms that conform to ethical and legal norms.

Globally, many jurisdictions have introduced regulatory frameworks, which India can take guidance from while formulating specific whistleblower protection laws for AI. Through legislation such as the Sarbanes-Oxley Act to protect corporate whistleblowers and the Algorithmic Accountability Act for AI-driven decision-making, the United States has created a strong regime for whistleblower protection. In a similar vein, the UK's Public Interest Disclosure Act provides robust whistleblower protections that cover all sectors (public and private), and its AI Regulation At a more granular level, the European Union's AI Act and General Data Protection Regulation (GDPR) also lay out comprehensive guidelines regarding AI governance and data privacy, complete with hard measures to ensure that AI solutions can be held to account and that algorithms remain free of bias. India may follow suit by introducing risk-based AI governance regulations and embedding AI-specific data protection measures in its whistleblower legislation. (Frontiers in Human Dynamics, n.d.)

Moving forward, incorporating AI into whistleblowing in India must adopt a collaborative approach involving all stakeholders including the government, corporations, and technology experts. Working closely amongst regulators, legal practitioners and AI builders will lend itself to the development of AI-fuelled fraud detection frameworks being aligned to standards of corporate governance and also preserving the rights of whistle-blowers. Building AI literacy amongst compliance officers and corporate governance professionals is a key enabler in the effective adoption of AI whistleblowing tools. Through the adoption of, comprehensive AI governance frameworks, improved regulatory oversight, and emphasis on the ethical deployment of AI, India can strengthen the credibility and efficacy of its whistleblowing mechanisms, leading to a culture of corporate transparency and accountability.

V. Conclusion

The incorporation of artificial intelligence (AI) into whistleblowing systems is a huge step towards improving corporate governance and detecting fraud. This research has examined the impact of AI-enabled fraud detection technology on the functioning of whistleblowing mechanisms, especially in India, and interrogated the moral, legal, and regulatory dimensions of introducing AI-based whistleblowing systems. The increasing prevalence of AI technologies like machine learning, predictive analytics, and natural language processing in detecting unlawful behavior and corporate malfeasance is highlighted by the study. By allowing real-time fraud detection, improving the accuracy of identifying and rectifying financial irregularities, and providing organizations with data-driven insights into corporate risk mitigation, these technological advances have strengthened whistleblower mechanisms. Some benefits however, AI whistleblowing systems come with serious issues and challenges around data privacy, algorithmic bias, ethical dilemmas, and concerns around regulatory framework all of which need to be resolved before implementing AI whistleblowing systems effectively.

In creating AI-based whistleblowing platforms in India there will be several suggestions. The first is a general need for a concrete legal framework that encompasses AI-led whistleblowing and fraud detection. Whistleblower protection regimes, such as the Whistle Blowers Protection Act, 2014, and SEBI regulations, must be amended or adopted to integrate provisions for AI; AI-based whistleblowing mechanisms must be embedded in legally sustainable structures. This also means that data protection laws need to be strengthened to protect the privacy and confidentiality of whistleblowers when sensitive corporate data is scanned through for AI systems. For example, a regulatory framework requiring transparency in AI decision-making processes based on the European Union's AI Act can strengthen accountability and deter the misuse of AI in whistleblowing. Second, organizations must implement best practices for the ethical application of AI to help bring fairness and reliability to whistleblowing systems. AI models need to be tested rigorously, so the biases and inaccuracies in such models are reduced, which in turn, reduces false positives and negatives for fraud. Additionally, Explainable AI (XAI) approaches can be integrated into whistleblowing platforms to ensure transparency in AI-based decisions and enable compliance officers and regulators to verify the authenticity of any AI language-based whistleblower reports. Furthermore, hybrid whistleblowing systems integrating AI-fueled analysis with human intervention can create a fair mechanism by which whistleblower reports can be treated with the thoroughness and context that they merit.

We need to balance the efficiency of AI with the best ethical practices so that the whistleblowing systems do not get compromised. AI can even boost fraud detection efforts, but it should never replace human intuition, particularly in the whistleblowing context. Such mechanisms so driven by AI have to be constructed with in-built constraints such that ethical concerns remain paramount and automation does not override the hallmark principles of whistleblowing, or prevent any unfair punishments of whistleblowers. Organizations need to adopt governance policies that are consistent with corporate ethics, promoting transparency, accountability, and fairness in AI-assisted whistleblowing.

AI-based whistleblowing offers a powerful opportunity to enhance corporate governance in India by improving fraud detection and promoting a culture of transparency. However, it must be optimally executed with a clear regulatory framework, ethical AI, and a balanced approach between technological efficiency and human oversight. By overcoming these challenges and implementing global best practices, India can create a strong AI-powered whistleblowing system that not only ensures the safety of whistleblowers but also increases corporate accountability, which will result in mainly ethical enterprises and sustainable economic development.

VI. References:

[1]Institute of Company Secretaries of India. (2023). *Decoding whistle blowing policies of Indian companies*. *Chartered Secretary*, 77. https://www.icsi.edu/media/webmodules/CSJ/December/18.pdf

[2]Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates. (2024). *The US government is using AI to detect potential wrongdoing*. https://www.skadden.com/insights/publications/2024/03/insights-special-edition/the-us-government-is-using-ai

[3]SQream. (2024). *The best machine learning algorithms for fraud detection*. https://sqream.com/blog/fraud-detection-machine-learning/

[4]IBM. (2024). *What is predictive analytics?* https://www.ibm.com/think/topics/predictive-analytics

[5]Shaw, J. (2024, February 4). *Using NLP to detect fraud in insurance claims*. Insurance Thought Leadership. https://www.insurancethoughtleadership.com/claims/using-nlp-detect-fraud-insurance-claims

[6] Dubey, S. (2022). Artificial intelligence in financial fraud detection: A case study of Indian banking sector. *Innovative Research Thoughts*, 8(4). https://doi.org/10.36676/irt.v8.i4.1503

[7]Infosys BPM. (n.d.). *Fraud detection technologies: Make AI and machine learning work for you*. Infosys Blogs. https://www.infosysbpm.com/blogs/bpm-analytics/financial-fraud-detection.html

[8] Zuckerman, J., & Stock, M. (2025, February 21). *How to report cyber, AI, and emerging technologies fraud and qualify for an SEC whistleblower award*. National Law Review. https://natlawreview.com/article/how-report-cyber-ai-and-emerging-technologies-fraud-and-qualify-sec-whistleblower

[9]Steward, M. (n.d.). *Using artificial intelligence to keep criminal funds out of the financial system*. Financial Conduct Authority. https://www.fca.org.uk/news/speeches/using-artificial-intelligence-keep-criminal-funds-out-financial-system

[10]Mondaq. (n.d.). *The Indian disposition on whistleblowing in a private company*. https://www.mondaq.com/india/directors-and-officers/1128912/the-indian-disposition-on-whistleblowing-in-a-private-company

[11]Government of India. (2013). *Companies Act, 2013* (No. 18, Acts of Parliament, 2013). https://www.mca.gov.in

[12]Securities and Exchange Board of India. (2015). *Listing Obligations and Disclosure Requirements Regulations, 2015*. https://www.sebi.gov.in

[13]Government of India. (2023). *Digital Personal Data Protection Act, 2023* (No. 29, Acts of Parliament, 2023). https://www.meity.gov.in

[14]European Data Protection Supervisor. (n.d.). *Whistleblowing*. https://www.edps.europa.eu/data-protection/data-protection/reference-library/whistleblowing_en

[15]Ministry of Personnel, Public Grievances & Pensions. (2024, December 12). *Parliament question: Delay in operationalizing the Whistleblower Protection Act, 2014*. Press Information Bureau. https://pib.gov.in/PressReleasePage.aspx?PRID=2083815

[16]Burman, A. (2023, October 3). *Understanding India's new data protection law*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law

[17]OneTrust. (n.d.). *Solutions for GDPR compliance*. https://www.onetrust.com/solutions/gdpr-compliance/

[18]Anura.io. (n.d.). *The hidden pitfalls of AI in fraud detection: False positives*. https://www.anura.io/fraud-tidbits/the-hidden-pitfalls-of-ai-in-fraud-detection-false-positives

[19]Planet Compliance. (n.d.). *AI fraud detection systems and compliance*. https://www.planetcompliance.com/ai-compliance/ai-fraud-detection-systems/

[20]Frontiers in Human Dynamics. (n.d.). *Ensuring fairness in AI-based whistleblowing: Addressing algorithmic bias and enhancing transparency*. *Frontiers in Human Dynamics*. https://www.frontiersin.org/journals/human-dynamics/articles/10.3389/fhumd.2024.1421273/full