The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CORPORATE WHISTLEBLOWING IN INDIA: EVALUATING THE EFFECTIVENESS OF LEGAL PROTECTION FOR WHISTLEBLOWERS IN EXPOSING CORPORATE MISCONDUCT

– Archisman Jana[1] and Hansika Badlani[2]

ABSTRACT

Corporate whistleblowing is widely regarded as one of the most effective early-warning mechanisms against fraud, but its effectiveness depends on the legal protection extended to those who speak. This paper evaluates whether the legal framework presently available in India protects corporate whistleblowers well enough to expose corporate misconduct. Adopting a doctrinal method supported by case studies of Satyam, ICICI Bank–Videocon, Infosys and Ranbaxy, the paper assesses the Companies Act 2013, the regulations of the Securities and Exchange Board of India (SEBI), the Whistle Blowers Protection Act 2014 and allied laws against six parameters: coverage, accessibility of reporting channels, protection from retaliation, remedies and enforcement, incentives, and oversight. The Indian position is compared with the Sarbanes-Oxley and Dodd-Frank regimes in the United States, the Public Interest Disclosure Act 1998 in the United Kingdom, and Directive (EU) 2019/1937.

The paper finds that the Indian framework is fragmented and compliance-oriented rather than rights-based. The vigil mechanism obligation applies only to specified classes of companies and promises 'safeguards' without an enforceable remedy; the Whistle Blowers Protection Act 2014 remains un-notified and, even if notified, is directed at public servants rather than private corporations; and SEBI's reward-based informant scheme is confined to insider trading. The paper recommends a dedicated and sector-wide statutory protection, a specialised adjudicatory forum with burden-shifting and interim relief, statutory safe harbours against defamation and

[1]Archisman Jana, B.A. LL.B. (Hons.), 4th Year, Amity University, Kolkata.

[2]Hansika Badlani, B.A. LL.B. (Hons.), 4th Year, Amity University, Kolkata.

confidentiality claims, stronger audit committee independence, and transparent reporting of whistleblower data, so that the constitutional commitment to transparency and the corporate law commitment to accountability are matched by a workable protection for those who expose wrongdoing.

Keywords: Whistleblowing, Corporate Governance, Vigil Mechanism, Companies Act 2013, SEBI, Retaliation, Whistle Blowers Protection Act 2014

INTRODUCTION

Corporations act through people, and wrongdoing inside a corporation is therefore most often known first to those who work within it. The accountant sees the manipulated entry, the procurement officer sees the inflated invoice, and the compliance officer sees the report that is quietly diluted before it reaches the board. Whistleblowing, which the leading definition in organisational studies describes as the disclosure by current or former members of an organisation of illegal, immoral or illegitimate practices under the control of their employers to persons or bodies that may be able to act on them,[3] is the channel through which that knowledge reaches those who can act upon it. In the vocabulary of Albert Hirschman, it is an exercise of 'voice' by insiders who might otherwise choose silence or 'exit'.[4]

Empirical work on fraud detection reinforces the point. The global study of occupational fraud conducted by the Association of Certified Fraud Examiners has repeatedly found that tips, a large share of which come from employees, are the most common way in which fraud is detected, ahead of internal audit and management review.[5] A study of corporate frauds in the United States by Dyck, Morse and Zingales found that employees, although an important source, were only one of several actors, alongside the media, auditors and analysts, that brought frauds to light.[6] A healthy disclosure system therefore needs several well-protected channels, not reliance on a single gatekeeper.

India's corporate experience illustrates both the cost of silence and the cost of speaking. The collapse of Satyam Computer Services in January 2009, after its chairman admitted in a letter

[3]Janet P Near and Marcia P Miceli, 'Organizational Dissidence: The Case of Whistle-Blowing' (1985) 4 Journal of Business Ethics 1, 4.

[4]Albert O Hirschman, *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States* (Harvard University Press 1970).

[5]Association of Certified Fraud Examiners, *Occupational Fraud 2024: A Report to the Nations* (ACFE 2024).

[6]Alexander Dyck, Adair Morse and Luigi Zingales, 'Who Blows the Whistle on Corporate Fraud?' (2010) 65 Journal of Finance 2213.

to the board that the company's accounts had been falsified over a period of years,[7] showed how a governance structure can appear sound until the moment it fails. In the public sector, the murder of National Highways Authority of India engineer Satyendra Dubey in November 2003, after he had written in confidence to the Prime Minister's Office about irregularities in a highway project, prompted the Supreme Court to direct the Government to create machinery for acting on such complaints.[8] Despite these episodes, India has no operative, sector-wide statute that protects corporate whistleblowers. The Whistle Blowers Protection Act 2014, which received Presidential assent on 9 May 2014,[9] has still not been brought into force,[10] and is in any event concerned with disclosures about public servants. Protection for the corporate whistleblower must instead be assembled from the Companies Act 2013, the SEBI regulations, sectoral regulator schemes, and the general law of employment, contract, tort and crime.

Statement of the Problem

A legal protection is effective only if it persuades people with knowledge of wrongdoing to come forward, shields them when they do, and results in the misconduct being investigated and corrected. The central problem addressed in this paper is whether the patchwork of Indian provisions meets that test in the corporate context, or whether it leaves the whistleblower exposed to dismissal, defamation claims and professional ruin while giving the corporation little incentive to take disclosures seriously.

Objectives and Research Questions

The paper has four objectives: first, to trace the evolution and present content of the Indian legal framework for corporate whistleblowing; second, to assess its effectiveness against defined parameters; third, to examine how India's framework compares with leading international models; and fourth, to propose reforms. The paper is guided by three questions. What legal protections are presently available to a person who exposes misconduct within a private corporation in India? How effective are those protections in practice, as revealed by

[7] Letter from B Ramalinga Raju, Chairman, Satyam Computer Services Ltd to the Board of Directors (7 January 2009), disclosed to the stock exchanges.

[8] *Centre for Public Interest Litigation v Union of India*, Writ Petition (Civil) No 539 of 2003 (SC).

[9] Whistle Blowers Protection Act 2014 (Act 17 of 2014). For the date of assent, see Prakriti Bhatt, 'Whistle Blowing: A Hobson's Choice?' (2019) 10 The Law Review, Government Law College 1.

[10] Khaitan & Co, 'Guide to Whistleblowing: India' (2026) <www.khaitanco.com> accessed 10 November 2026; see also 'Changes in Whistle Blowers Protection Act not part of business of current Parliament session: Centre' *ThePrint* (4 December 2024).

prominent corporate episodes? What reforms are needed to align Indian law with constitutional values and international standards?

Hypothesis

The paper proceeds on the hypothesis that the existing Indian framework, being fragmented, compliance-driven and lacking an enforceable anti-retaliation remedy, is inadequate to protect corporate whistleblowers and therefore falls short of exposing corporate misconduct effectively.

Research Methodology and Limitations

The study is doctrinal and analytical. It relies on primary sources (statutes, rules, regulations and judicial decisions) and secondary sources (reports of expert bodies, journal articles, regulatory publications and company disclosures). The case studies are drawn from publicly available information and are used to illustrate structural features of the framework, not to adjudicate the truth of any allegation. No primary empirical data, such as surveys or interviews with whistleblowers, has been collected, and Indian companies do not publish consolidated whistleblower statistics; conclusions about practice are therefore inferential. The law is stated as understood on 10 November 2026.

CONCEPTUAL AND THEORETICAL FOUNDATIONS

Meaning and Forms of Corporate Whistleblowing

Whistleblowing is distinct from an ordinary workplace grievance. A grievance concerns the complainant's own terms of employment, whereas a whistleblowing disclosure concerns wrongdoing that affects others, such as shareholders, creditors, consumers, the exchequer or the public. Disclosures may be *internal*, made to management, the audit committee or an ethics hotline, or *external*, made to a regulator, law-enforcement agency, the media or civil society. The distinction matters legally because many regimes, including those of India, privilege internal reporting, while the effectiveness of internal channels depends on the independence of those who receive the report. In the corporate setting, protected subject-matter typically includes accounting and financial-reporting fraud, bribery and corruption, insider trading and market manipulation, violation of regulatory conditions, and serious safety or environmental breaches.

Why the Law Must Protect the Whistleblower

Three justifications support legal protection. The first is economic. Modern companies separate ownership from control, so shareholders cannot directly observe what managers do, and the resulting information asymmetry is the central agency problem of corporate law.[11] A whistleblower is a low-cost source of information that reduces this asymmetry. The second is constitutional. The Supreme Court has read a right to know into Article 19(1)(a) of the Constitution, first in the context of governmental acts[12] and later in relation to corporate affairs of public concern,[13] and a person who risks livelihood to supply such information advances that right. The third is international. Article 33 of the United Nations Convention against Corruption invites States Parties to consider appropriate measures to protect persons who report corruption in good faith, and India ratified the Convention in 2011.[14]

Against these justifications stand the legitimate interests of the corporation. Employees owe duties of loyalty and confidentiality, false allegations can destroy reputations and depress share prices, and a protection regime that rewards malicious complaints would be abused. An effective framework must therefore protect good-faith disclosure while deterring knowingly false or malicious complaints.

Parameters for Evaluating Effectiveness

This paper evaluates the Indian framework against six parameters that recur in comparative scholarship and in international standards: (i) *coverage*, meaning who is protected and for what disclosures; (ii) *accessibility of channels*, meaning whether credible internal and external routes exist; (iii) *protection from retaliation*, including confidentiality and safeguards against dismissal and harassment; (iv) *remedies and enforcement*, meaning whether a retaliated-against whistleblower has a forum, relief and a lighter burden of proof; (v) *incentives*, meaning whether the system encourages disclosure; and (vi) *oversight*, meaning whether the system generates data and is accountable.

[11] Michael C Jensen and William H Meckling, 'Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure' (1976) 3 Journal of Financial Economics 305.

[12] *State of Uttar Pradesh v Raj Narain* (1975) 4 SCC 428.

[13] *Reliance Petrochemicals Ltd v Proprietors of Indian Express Newspapers Bombay Pvt Ltd* (1988) 4 SCC 592.

[14] United Nations Convention against Corruption (adopted 31 October 2003, entered into force 14 December 2005) 2349 UNTS 41, art 33.

EVOLUTION OF THE INDIAN LEGAL FRAMEWORK

India's approach to whistleblowing developed in reaction to scandals, not through planned design. In *Vineet Narain v Union of India*, arising from the investigation of the 'Jain Hawala' case, the Supreme Court laid down directions to insulate investigative agencies from executive interference and to give statutory status to the Central Vigilance Commission (CVC).[15] The institutional groundwork for receiving complaints was thus laid before any law protected the person who made them. The Law Commission of India, in its 179th Report in 2001, recommended a statute on public interest disclosure and protection of informers.[16]

The corporate sector received attention shortly afterwards. The Committee on Corporate Governance chaired by N R Narayana Murthy recommended in 2003 that a whistle blower policy be adopted by listed companies,[17] and the revised Clause 49 of the Listing Agreement incorporated it as a non-mandatory requirement. The Ministry of Corporate Affairs later included a whistle blower policy in its voluntary Corporate Governance Guidelines of 2009.[18] The murder of Satyendra Dubey led to the Public Interest Disclosure and Protection of Informers Resolution of 2004, which designated the CVC as the agency to receive complaints against central government employees and certain public bodies and promised protection from victimisation.[19] The Resolution was an executive instrument, limited to the public sector, and had no statutory force.

The Satyam fraud of 2009 shifted the debate to private companies. The Companies Act 2013 made a vigil mechanism mandatory for specified classes of companies; Parliament enacted the Whistle Blowers Protection Act in 2014; and SEBI, between 2018 and 2019, required listed companies to maintain whistleblower policies for the leakage of unpublished price sensitive information and created a reward-based informant mechanism for insider trading. The sequence shows steady expansion of obligations, but also that each step addressed a single segment of the problem.

---

[15] *Vineet Narain v Union of India* (1998) 1 SCC 226.

[16] Law Commission of India, *179th Report on The Public Interest Disclosure and Protection of Informers* (December 2001).

[17] Securities and Exchange Board of India, *Report of the SEBI Committee on Corporate Governance* (February 2003).

[18] Ministry of Corporate Affairs, *Corporate Governance Voluntary Guidelines 2009* (December 2009).

[19] Government of India, Public Interest Disclosure and Protection of Informers Resolution (21 April 2004).

THE PRESENT LEGAL FRAMEWORK FOR CORPORATE WHISTLEBLOWERS

The Companies Act 2013

Section 177(9) requires every listed company, and such other class of companies as may be prescribed, to establish a vigil mechanism for directors and employees to report genuine concerns. Section 177(10) adds that the mechanism shall provide adequate safeguards against victimisation of persons who use it and make provision for direct access to the chairperson of the audit committee in appropriate or exceptional cases.[20] The prescribed classes, under Rule 7 of the Companies (Meetings of Board and its Powers) Rules 2014, are companies that accept deposits from the public and companies that have borrowed from banks and public financial institutions in excess of fifty crore rupees.[21] Separately, section 143(12) obliges an auditor who has reason to believe that an offence involving fraud is being or has been committed against the company by its officers or employees to report the matter, to the Central Government where the amount involved is one crore rupees or more and otherwise to the audit committee or the Board.[22]

The provisions are significant because they place a structural duty on the company itself. Their limits are discussed below. The statute does not define ‘victimisation’, does not create a cause of action for a person victimised, does not shift the burden of proof, and does not prescribe a remedy. Non-compliance is left to the general residual penalty provision of the Act.[23]

SEBI Regulations

Under the SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, a listed entity must devise an effective whistle blower mechanism enabling stakeholders, including individual employees and their representative bodies, to communicate concerns about illegal or unethical practices freely,[24] and must formulate a vigil mechanism for directors and employees, with safeguards against victimisation and direct access to the audit committee chairperson in appropriate cases.[25] The Regulations are broader than the Companies Act in

[20]Companies Act 2013, s 177(9)–(10).

[21]Companies (Meetings of Board and its Powers) Rules 2014, r 7.

[22]Companies Act 2013, s 143(12); Companies (Audit and Auditors) Rules 2014, r 13.

[23]Companies Act 2013, s 450.

[24]Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations 2015, reg 4(2)(d)(iv).

[25]ibid reg 22.

using the language of 'stakeholders', but the operative vigil mechanism is still confined to directors and employees.

The SEBI (Prohibition of Insider Trading) Regulations 2015 contain two further layers. Regulation 9A(6), effective from 1 April 2019, requires listed companies to have a whistleblower policy so that employees can report instances of leakage of unpublished price sensitive information.[26] Chapter IIIA, inserted with effect from 26 December 2019, creates an informant mechanism under which an individual who submits original information about insider trading through a Voluntary Information Disclosure Form to SEBI's Office of Informant Protection may be rewarded where monetary sanctions are collected, with the reward capped at one crore rupees or such higher amount as SEBI may specify, and the regulations prohibit retaliation and protect the informant's confidentiality.[27] This is the only monetary reward scheme for whistleblowers in Indian securities law, and it is limited to a single category of violation.

Sectoral Schemes

Regulators of specific sectors have issued their own arrangements. The Reserve Bank of India, for example, has operated a Protected Disclosures Scheme for private sector and foreign banks since 2007, under which complaints may be made to the Reserve Bank itself.[28] Such schemes provide an external channel, but they are administrative in nature and do not confer a judicially enforceable right on the complainant.

The Whistle Blowers Protection Act 2014

The Act establishes a mechanism for receiving and inquiring into public interest disclosures relating to allegations of corruption, wilful misuse of power or discretion, or criminal offences by public servants, designates competent authorities such as the CVC, and provides for protection against victimisation and for penalties for false or frivolous complaints.[29] Three features limit its relevance to corporate misconduct. First, its subject matter is conduct of public servants, so it covers private corporations only incidentally. Second, it has never been notified under section 1(3) of the Act. Third, the Whistle Blowers Protection (Amendment) Bill 2015,

[26]Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations 2015, reg 9A(6), inserted by the Securities and Exchange Board of India (Prohibition of Insider Trading) (Amendment) Regulations 2018.

[27]ibid ch IIIA, regs 7A–7M, inserted by the Securities and Exchange Board of India (Prohibition of Insider Trading) (Third Amendment) Regulations 2019 (notified 17 September 2019).

[28]Reserve Bank of India, Protected Disclosures Scheme for Private Sector and Foreign Banks (2007).

[29]Whistle Blowers Protection Act 2014 (Act 17 of 2014), long title and statement of objects and reasons.

passed by the Lok Sabha in May 2015, proposed to bar disclosures falling within categories of information exempted under section 8(1) of the Right to Information Act 2005, a restriction that critics argued would weaken the Act,[30] and the Government stated in December 2024 that amendments were not part of the legislative business of the session.[31] The Act also does not entertain disclosures that do not disclose the identity of the complainant.[32]

General Law

In the absence of a dedicated remedy, the whistleblower must rely on general law. The relevant labour law is now the Industrial Relations Code 2020, which came into force on 21 November 2025 and replaced the Industrial Disputes Act 1947.[33] That law protects 'workers', a category that has traditionally excluded persons employed mainly in managerial or administrative roles, who are likely to be those with access to financial and strategic information. For persons outside it, remedies lie in contract, where the Supreme Court has recognised that terms of employment may be struck down as unconscionable, although in a case involving a public sector corporation.[34] Constitutional writ remedies are principally available against the State and its instrumentalities,[35] although Article 226 permits writs against private bodies that discharge public functions.[36]

The general criminal law also operates against the whistleblower. Defamation is an offence under section 356 of the Bharatiya Nyaya Sanhita 2023, which replaced section 499 of the Indian Penal Code 1860,[37] and corporations can bring civil suits for damages and injunctions, a risk well suited to intimidating individuals who cannot afford protracted litigation. On the protective side, section 398 of the Bharatiya Nagarik Suraksha Sanhita 2023 requires each State to notify a witness protection scheme, which a whistleblower who becomes a witness may

[30]Whistle Blowers Protection (Amendment) Bill 2015; see Venkatesh Nayak, 'Government's ominous signals on Whistle Blower Protection Act' *Law and Other Things* <https://lawandotherthings.com> accessed 10 November 2026.

[31]'Govt says amendment to Whistle Blowers Protection Act not in agenda of current Parliament session: Report' *The Wire* (5 December 2024).

[32]Whistle Blowers Protection Act 2014, s 4.

[33]Industrial Relations Code 2020 (Act 35 of 2020), brought into force on 21 November 2025; Industrial Relations Code (Amendment) Act 2026.

[34]*Central Inland Water Transport Corporation Ltd v Brojo Nath Ganguly* (1986) 3 SCC 156.

[35]*Ajay Hasia v Khalid Mujib Sehravardi* (1981) 1 SCC 722.

[36]*Andi Mukta Sadguru Shree Muktajee Vandas Swami Suvarna Jayanti Mahotsav Smarak Trust v V R Rudani* (1989) 2 SCC 691.

[37]Bharatiya Nyaya Sanhita 2023, s 356.

invoke,[38] and the Prevention of Corruption Act 1988, as amended in 2018, now makes a commercial organisation liable for bribery by persons associated with it, subject to a defence of adequate procedures, which gives companies a compliance reason to maintain credible reporting channels.[39] The same amendment inserted section 17A, which requires prior approval before an inquiry or investigation into decisions taken by public servants in the discharge of official functions, which may add a procedural hurdle where corporate misconduct involves public officials.[40]

CASE STUDIES: WHAT PRACTICE REVEALS

The cases below are not a representative sample. They are chosen because each exposes a different dimension of the framework, and the paper draws no conclusions as to the merits of any allegation beyond what the cited sources record.

Satyam Computer Services (2009)

Satyam is often cited as the origin of modern Indian corporate governance reform. Its relevance to whistleblowing is, paradoxically, that the fraud did not emerge through a whistleblower or a vigil mechanism. It emerged through the confession of the chairman.[41] The company, a listed entity with an audit committee and independent directors, had a formal governance architecture, yet the structure did not surface the problem. This illustrates the limit of regimes that rely on directors and audit committees as the sole recipients of concerns when management itself is the source of the wrongdoing.

ICICI Bank and the Videocon Loans (2016–2018)

In March 2016, Arvind Gupta, a shareholder of both ICICI Bank and the Videocon Group, wrote to the Prime Minister, the Reserve Bank of India and other authorities alleging a conflict of interest in loans extended by the bank to the Videocon Group.[42] The bank's board commissioned an inquiry by a law firm that initially found no basis for the allegations, and the board publicly expressed its full confidence in the Chief Executive Officer.[43] Following further

[38] Bharatiya Nagarik Suraksha Sanhita 2023, s 398.

[39] Prevention of Corruption Act 1988, s 9, inserted by the Prevention of Corruption (Amendment) Act 2018.

[40] ibid s 17A.

[41] Raju (n 7).

[42] 'Why Arvind Gupta Questioned Videocon-ICICI Bank Dealings in 2016' *The Quint* <https://www.thequint.com> accessed 10 November 2026.

[43] 'ICICI Bank: Top Law Firm Cyril Amarchand Mangaldas Withdraws Report That Cleared Kochhar' *BloombergQuint* (October 2018).

anonymous complaints in 2018, the board appointed Justice B N Srikrishna, a former Judge of the Supreme Court, to examine the matter, the Chief Executive Officer resigned in October 2018, and the earlier legal opinion was withdrawn.[44]

Three lessons follow. First, the original complainant was a shareholder, a person who falls outside the statutory vigil mechanism for 'directors and employees', and was left to write to the Prime Minister and regulators with no formal channel or protection. Second, the board's initial inquiry was conducted under the supervision of the company's own chairperson, illustrating the conflict inherent in internal investigation of allegations against the top executive. Third, the matter acquired momentum only after the issue entered the public domain through the press and further complaints, which suggests that internal vigil mechanisms may be least reliable precisely where the allegation concerns the most senior management.

Infosys (2019–2020)

In October 2019, Infosys disclosed that it had received anonymous whistleblower complaints, from a group describing itself as 'ethical employees', alleging unethical practices by its Chief Executive Officer and Chief Financial Officer. The audit committee, assisted by an external law firm and an accounting firm, investigated, and in January 2020 concluded that the allegations were substantially without merit and that no restatement of financial statements was warranted.[45] The US Securities and Exchange Commission later informed the company that it had concluded its investigation and did not anticipate further action.[46]

The Infosys episode is useful for what it shows about the other side of the balance. The allegations were investigated and not substantiated, yet the disclosure was followed by a sharp fall in the share price, and the stock exchange asked the company to explain why the complaint had not been disclosed earlier under regulation 30 of the SEBI (LODR) Regulations.[47] It demonstrates both the value of a functioning audit committee process and the reputational and market consequences of unverified anonymous allegations, and thus the need for a framework that separates good-faith disclosure from malicious complaints, protects the identity of genuine

[44]'ICICI Bank to probe CEO Kochhar' *Business Standard* (31 May 2018); 'Credibility crisis' *The Week* (8 February 2019).

[45]Infosys Ltd, Press Release, 'Infosys Audit Committee Finds No Evidence of Financial Impropriety or Executive Misconduct' (10 January 2020).

[46]'Infosys Whistleblower Case: SEC Probe Over, No Further Action' *The Quint* (24 March 2020).

[47]'Nandan Nilekani defends Infosys concealing whistleblower's complaints' *India TV* (2019).

complainants, and sets clear rules about when and how complaints must be disclosed to the market.

Ranbaxy (2013)

Ranbaxy, then a leading Indian pharmaceutical company, pleaded guilty in the United States in 2013 to felony charges relating to the manufacture and distribution of certain adulterated drugs and to false statements to the US Food and Drug Administration, and agreed to pay five hundred million dollars to resolve criminal and civil liability.[48] The matter began with disclosures by a former senior employee to the US regulator and was pursued through the US enforcement machinery. The case is instructive because the corporate misconduct of an Indian company was exposed and sanctioned through foreign institutions, and the protective and compensatory infrastructure on which a whistleblower of that kind could rely was American, not Indian.

COMPARATIVE PERSPECTIVES

United States

The Sarbanes-Oxley Act 2002 requires audit committees of listed companies to establish procedures for the receipt, retention and treatment of complaints regarding accounting and auditing matters, including confidential and anonymous submissions by employees,[49] and section 806 prohibits retaliation against employees of listed companies who report suspected fraud, with remedies that include reinstatement, back pay and compensation for special damages.[50] The Dodd-Frank Act 2010 added a bounty programme under which the Securities and Exchange Commission pays eligible whistleblowers between ten and thirty per cent of monetary sanctions exceeding one million dollars.[51] The US Supreme Court has limited the Dodd-Frank anti-retaliation provision to persons who have reported to the Commission,[52] which illustrates that even a mature system faces difficult drafting questions about who is protected.

[48]United States Department of Justice, 'Generic Drug Manufacturer Ranbaxy Pleads Guilty and Agrees to Pay $500 Million to Resolve False Claims Allegations, cGMP Violations and False Statements to the FDA' (Press Release, 13 May 2013).

[49]Sarbanes-Oxley Act 2002, Pub L 107-204, s 301.

[50]ibid s 806 (18 USC § 1514A).

[51]Dodd-Frank Wall Street Reform and Consumer Protection Act 2010, s 922 (15 USC § 78u-6).

[52]*Digital Realty Trust Inc v Somers* 583 US 149 (2018).

United Kingdom

The Public Interest Disclosure Act 1998 inserted into the Employment Rights Act 1996 a tiered scheme under which workers who make a 'protected disclosure' to their employer, a prescribed regulator or, in defined circumstances, more widely, are protected against dismissal and detriment.[53] A worker may bring a claim before an employment tribunal, and compensation for such claims is not subject to the statutory cap that applies to ordinary unfair dismissal. The UK model is notable for its wide definition of 'worker' and for placing the remedy in an accessible specialist forum.

European Union

Directive (EU) 2019/1937 requires Member States to protect persons who report breaches of EU law in specified areas. It extends protection to a wide personal scope that includes employees, self-employed persons, shareholders, volunteers, trainees and contractors, requires internal and external reporting channels, protects confidentiality of the reporter, prohibits retaliation, shields reporters from liability for breach of confidentiality restrictions where they had reasonable grounds to believe that the report was necessary, and shifts the burden of proof to the person who took the detrimental measure.[54]

Lessons for India

Three features of the comparative models are especially relevant. First, protection is attached to the person and to a recognised channel, not to the existence of a corporate policy. Second, the burden of proof and the choice of forum are designed around the fact that the employer controls the evidence. Third, protection extends beyond employees to those closest to the corporate information flow. India's framework is weakest at exactly these points.

EVALUATING EFFECTIVENESS: AN ANALYSIS

The table below summarises the Indian position against the six parameters and the comparative benchmarks discussed above. It is followed by a discussion of the principal gaps.

[53]Employment Rights Act 1996, pt IVA (ss 43A–43L), ss 47B and 103A, inserted by the Public Interest Disclosure Act 1998.

[54]Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law [2019] OJ L305/17, arts 4, 16, 21.

Parameter	India (present position)	Comparative benchmark
Coverage	Directors and employees of listed and prescribed companies (Companies Act s 177; LODR reg 22). WBPA covers disclosures about public servants. Unlisted and smaller companies largely outside.	US: employees and contractors of public companies. EU: employees, contractors, shareholders, volunteers and others (art 4).
Reporting channels	Internal vigil mechanism with access to audit committee chair; SEBI informant channel for insider trading; sectoral schemes (RBI).	EU: internal and external channels plus public disclosure in defined cases. US: direct reporting to SEC.
Protection from retaliation	Statutory language of 'adequate safeguards'; no defined remedy, no burden-shifting; SEBI Chapter IIIA prohibits retaliation for insider-trading informants.	US (SOX s 806): reinstatement, back pay, special damages. UK: tribunal claim for dismissal or detriment. EU: burden of proof on employer (art 21).
Remedies and enforcement	No dedicated forum. Resort to civil court, labour forum (for 'workers') or writ jurisdiction. Residual fine for non-compliance.	UK: employment tribunal with uncapped compensation. US: administrative complaint and court action.
Incentives	Monetary reward only for insider trading information (SEBI).	US (Dodd-Frank): 10–30% of sanctions above USD 1 million.
Oversight and data	No consolidated public data on complaints or outcomes; WBPA oversight inoperative.	EU: Member State reporting of statistics (art 27). US: SEC reports to Congress.

Coverage Gaps

The vigil mechanism obligation in the Companies Act reaches listed companies and the prescribed classes only, leaving a large part of India's corporate sector, including many unlisted companies, limited liability partnerships and start-ups, outside any statutory reporting duty. Even where the duty applies, it speaks of 'directors and employees', leaving out ex-employees, contractors, consultants, suppliers and shareholders. The ICICI Bank episode shows that the first person to raise a serious concern may be a shareholder. The LODR Regulations' reference to 'stakeholders' is welcome, but it appears in the statement of principles and is not matched by an enforceable channel and protection.

Dependence on the Company's Self-Regulation

The architecture is largely one of internal compliance. The channel is operated by the company, the receiving authority is the company's audit committee, and the investigation is often

commissioned by the company's board from advisers it selects. When the allegation concerns a mid-level irregularity, that structure may work adequately. When it concerns the chief executive, the chairperson or the controlling shareholder, as in the ICICI Bank and Infosys episodes, the system depends on the independence and courage of the audit committee. The law supplies safeguards of form, such as direct access to the audit committee chairperson, but supplies no external check on how the matter is handled.

The Missing Remedy

The most serious deficiency is the absence of an enforceable anti-retaliation remedy. A promise of 'adequate safeguards against victimisation' without a cause of action, a forum, interim relief or a rule on the burden of proof leaves the whistleblower to prove, in an ordinary civil court or labour forum, that a dismissal or demotion was motivated by the disclosure, while the employer controls the documents and can usually advance an unrelated performance rationale. The reach of labour law is limited to 'workers', which excludes senior employees, and constitutional remedies are, in the main, available against the State. The effect is that the persons best positioned to detect financial misreporting, such as finance, audit and compliance professionals, are the least well protected.

Legal Risks Unaddressed

Defamation, breach of confidentiality and non-disclosure covenants, and claims of misuse of company data are risks that a whistleblower must weigh. Indian law does not provide a statutory safe harbour for good-faith disclosures to designated authorities, in contrast with the EU Directive. The risk is compounded for anonymous complainants, who are not entertained under the Whistle Blowers Protection Act, and who in corporate settings may be exposed to forensic efforts to identify them.

Incentives and Oversight

SEBI's informant reward is a welcome departure, but it is limited to insider trading. A person who discloses accounting fraud, bribery or diversion of funds has no comparable reward in securities or company law and may risk their career with no prospect of compensation. At the same time, the regulatory architecture generates little information about how the system works. Companies are not required to disclose, in a consolidated manner, the number of complaints received, their category and outcome, and no authority publishes aggregate data, so that neither the legislature nor the public can assess effectiveness.

Testing the Hypothesis

The analysis supports the hypothesis. The framework is fragmented across statutes and regulations, concentrates on obliging companies to maintain mechanisms rather than on giving individuals enforceable rights, and falls short on the parameters of coverage, remedies, incentives and oversight. The Companies Act and SEBI provisions have undoubtedly improved the formal infrastructure of reporting, and the SEBI informant scheme shows that targeted reform is possible. Their effect on actual exposure of misconduct cannot be quantified without data, but the case studies suggest that major corporate controversies continue to surface through press reports, regulators and shareholders as often as through internal channels.

RECOMMENDATIONS

A Dedicated and Sector-Wide Statutory Protection

Parliament should either notify the Whistle Blowers Protection Act 2014 after correcting its deficiencies, or enact a separate statute, or an enlarged chapter in the Companies Act 2013, specifically protecting persons who disclose corporate misconduct. The legislation should apply to all companies above a prescribed size and to limited liability partnerships, define ‘whistleblower’ to include current and former employees, directors, contractors, suppliers and shareholders, and define protected disclosure by reference to a reasonable belief and not to proof of wrongdoing. The restrictive amendments proposed in 2015 should not be adopted as drafted.

Enforceable Anti-Retaliation Rights and a Specialised Forum

The law should expressly prohibit dismissal, demotion, harassment, blacklisting and other detriment for making a protected disclosure, and provide that once the whistleblower establishes that a protected disclosure was made and a detriment followed, the burden shifts to the employer to show that the action was unrelated. Remedies should include interim relief, reinstatement, back wages and compensation. A specialised forum, whether a designated bench of the National Company Law Tribunal, the labour adjudicatory bodies under the Industrial Relations Code, or a new whistleblower authority, should be empowered to grant such relief expeditiously, regardless of whether the complainant is a ‘worker’ or a managerial employee.

Statutory Safe Harbour and Protection of Identity

A good-faith disclosure to the audit committee, a designated regulator or a law-enforcement authority should be immune from civil and criminal liability for defamation, breach of confidentiality and non-disclosure obligations. Contractual terms purporting to waive

whistleblower protection should be void. Rules on confidentiality of identity, modelled on SEBI's informant regulations, should apply across the framework, and anonymous disclosures should be accepted for preliminary scrutiny, with penalties for knowingly false or malicious complaints to protect against misuse.

Strengthening Internal Governance

Complaints against the chief executive, whole-time directors, promoters or members of the audit committee should be routed directly to the chairperson of the audit committee or, where the chairperson is implicated, to the lead independent director, and investigated by counsel independent of management. The audit committee should report to the board quarterly on complaints received and action taken, and listed companies should disclose in their annual report the number and categories of complaints and their disposition, along with the number of retaliation allegations. Clear rules should also govern disclosure to the exchanges of material complaints, balancing the market's right to know against the risk of damage from unverified allegations.

Wider Incentives and Regulatory Coordination

SEBI should consider extending its informant reward scheme beyond insider trading to serious securities-law frauds, with safeguards against abuse. The Ministry of Corporate Affairs, SEBI, the Reserve Bank of India and the Serious Fraud Investigation Office should adopt a coordinated protocol for receiving and cross-referring disclosures, so that a whistleblower is not required to identify the correct regulator before obtaining protection, and so that an Indian whistleblower does not have to rely on foreign institutions, as in the Ranbaxy matter.

Training, Culture and Data

Law cannot substitute for organisational culture. Companies should train managers in receiving concerns, and regulators should publish annual aggregate statistics on disclosures, outcomes and retaliation claims. Such data would also enable the empirical evaluation which this paper could not undertake.

CONCLUSION

Whistleblowers are among the few actors who can see corporate wrongdoing before it becomes a collapse. The Indian legal system has recognised their value in a series of incremental steps, from the Public Interest Disclosure Resolution of 2004 to the vigil mechanism of the Companies Act 2013 and the SEBI informant scheme of 2019. Yet these steps have created a structure that obliges companies to maintain reporting channels without giving whistleblowers

dependable rights. The Whistle Blowers Protection Act 2014 has remained dormant for more than twelve years, and the private sector whistleblower is left to a combination of internal policy, residual labour law and the risk of litigation.

The evaluation in this paper shows that the present framework is only partly effective. It succeeds in normalising the idea of an internal reporting channel and, in the case of insider trading, in providing an external route with incentives. It fails to protect those who are most exposed, to offer a forum and a fair burden of proof when retaliation occurs, to shield good-faith disclosure from defamation and confidentiality claims, and to generate data on its own performance. Reform of the kind proposed here would not eliminate corporate wrongdoing, but it would make it safer for those who see it to speak, and for the company to listen. That is the standard against which the effectiveness of whistleblower law must finally be measured.