International Journal of Juridical Studies & Research (IJJSR), Vol. 1, Issue 2, December 2024 Page 151 - 168

PROTECTING WHISTLEBLOWERS IN INDIAN WORKPLACES: LEGAL FRAMEWORK AND CHALLENGES

Rohit Tamang[1]

Diwash Saibya[2]

Abstract

Whistleblowers play a significant role in promoting transparency and accountability in organizations, particularly in identifying corruption, fraud, and unethical practices. In India, there exist legislative measures such as the Whistle Blowers Protection Act, 2014, intended to protect individuals who disclose improper practice in public and private organizations. Despite such legislation, several barriers persist, varying from fear of retaliation to low levels of awareness and poor enforcement mechanisms. Hierarchical pressures, organizational culture, and confidentiality issues deter employees further from making disclosures on unethical practices. Also, vagaries of the definition of protected disclosures and procedural delays often erode the effectiveness of legal safeguards. This article examines India's current legislative and regulatory framework for the protection of whistleblowers, assessing their scope, limitations, and actual application. The importance of corporate governance, in-house reporting systems, and ethics-based leadership in creating a culture of responsibility is also examined. Comparative observations from international best practices suggest methods by which protection can be enhanced and reporting can be promoted. The study emphasizes the need for comprehensive policy, awareness-raising programs, and autonomous auditing institutions to mitigate threats to whistleblowers and promote an open work culture. By removing legal, organizational, and socio-cultural barriers, India can transition towards a more accountable and integrity-oriented workplace system.

[1] B.COM, LL.B.), INDIAN INSTITUTE OF LEGAL STUDIES, UNIVERSITY OF NORTH BENGAL, LL.M. (CONSTITUTIONAL LAW), RESEARCHER

[2] B.A. LL.B. (HONS.), INDIAN INSTITUTE OF LEGAL STUDIES, UNIVERSITY OF NORTH BENGAL; PURSUING LL.M. (HUMAN RIGHTS AND DEVELOPMENT), FACULTY OF LAW, BANARAS HINDU UNIVERSITY, VARANASI

Keywords: *whistleblower protection, indian workplaces, legal structure, accountability, organizational ethics, retaliation, transparency.*

1. INTRODUCTION

WHISTLEBLOWING entails an insider reporting information on conduct that is **"illegitimate, illegal, or unethical"** and potentially threatening to the public interest.[3] In India, a traditional differentiation is drawn between "internal" disclosures, which are made through employer-designated channels, and "external" disclosures, which are addressed to regulatory authorities, oversight bodies, or the press.[4] Such categorization has been formalized in the Companies Act, 2013, and the SEBI (Listing Obligations & Disclosure Requirements) Regulations, 2015.[5] Whistleblowing is crucial to democratic governance, since empirical evidence in twenty-seven jurisdictions reveals that 43% of corporate frauds are detected by employee tips, a figure much higher compared to frauds discovered by audits (15%) or board monitoring (11%).[6] Through encouraging transparency, whistleblowers reduce information asymmetries, discourage rent-seeking activities, and lower the cost of capital for firms with effective speak-up processes.[7] Conversely, the lack of whistleblowers is correlated with higher levels of corruption and systemic abuse of markets.[8]

India's history demonstrates this phenomenon. The 2G spectrum scam, which caused an estimated loss to the exchequer of INR 1.76 trillion,[9] and the Satyam Computers accounting scam, worth INR 71.36 billion,[10] were first highlighted by internal auditors and junior engineers. Though their issues were first overlooked, they later triggered parliamentary probes, Supreme Court action, and major statutory changes. But these instances also showed that there was no

---

[3] Kohn, Kohn & Colapinto, Whistleblower Law: A Guide to Legal Protections for Corporate Employees 3 (2004)

[4] Organisation for Economic Co-operation & Development, OECD Study on Whistleblower Protection Frameworks, Compendium of Best Practices 12 (2021)

[5] Companies Act, 2013, § 177(9) & § 149(12); Securities & Exchange Board of India, LODR Regulations, 2015, Reg. 30(6) & Part A of Schedule III

[6] Association of Certified Fraud Examiners, Report to the Nations: 2022 Global Study on Occupational Fraud & Abuse 12

[7] Dyck, Morse & Zingales, Who Blows the Whistle on Corporate Fraud?, 65 J. Fin. 2213, 2233 (2010)

[8] Rose-Ackerman, Corruption and Government: Causes, Consequences and Reform 89 (1999)

[9] Comptroller & Auditor-General of India, Performance Audit Report on Issue of Licences and Allocation of 2G Spectrum 41-42 (2010)

[10] Securities & Exchange Board of India, Order in the Matter of Satyam Computer Services Ltd., WTM/GM/EFD/06/2009 (5 Jan. 2009)

protection for whistleblowers: Satyam whistleblower B. Ramalinga Raju's subordinates were sued for criminal defamation[11] and 2G petitioner S. P. Singh was compulsorily retired.[12] The Law Commission of India therefore concluded that the "absence of an institutional shield, chills disclosure and perpetuates maladministration."[13]

The legislative reaction has been piecemeal. The Whistle Blowers Protection Act, 2011, passed in response to the assassination of NHAI engineer Satyendra Dubey,[14] is still not notified for corporate-sector disclosures[15] and the pending 2015 Amendment Bill would limit the definition of "disclosure" and add a precondition of prior government approval.[16] Sections in the Companies Act, 2013 (§§ 177 & 149) and SEBI LODR only require internal ombudsmen, with external avenues left piecemeal.[17] Such uncertainty caused a 73% year-on-year fall in SEBI whistleblower complaints between 2019 and 2022,[18] to back survey data that 68% of Indian employees would still "rather keep quiet."[19] This paper therefore reviews the existing framework of statutes, regulation, and judicial protection; identifies enforcement issues of identity leakage, delayed investigations, and retaliatory litigation; and suggests reforms, including statute harmonization, creation of an independent Whistleblower Protection Authority, bounty-linked incentives, and Anti-SLAPP legislation, to enhance the framework foreseen by the 2011 Act.

1. CONCEPTUAL AND THEORETICAL FRAMEWORK

Whistleblowing is best analysed as a complicated governance phenomenon that occurs at the intersection of moral philosophy, agency economics, and public-regulatory theory. From the utilitarian point of view, whistleblowing is regarded

---

11 C. R. Sukumar, Satyam Whistle-blower Still Out of Job, LiveMint (13 Jan. 2009)

12 S. P. Singh v. Union of India, (2012) 3 SCC 288

13 Law Commission of India, Report No. 179, Public Interest Disclosure and Protection of Informers 7 (2001)

14 Satyendra Dubey, a project director at NHAI, was murdered after complaining to the Prime Minister's Office; the incident catalysed the 2004 Public Interest Disclosure Bill

15 Whistle Blowers Protection Act, 2011, received Presidential assent on 9 May 2014 but § 1(2) has never been brought into force for corporate disclosures; see Ministry of Personnel, Public Grievances & Pensions, Lok Sabha Unstarred Q. No. 3551 (14 Mar. 2022)

16 Whistle Blowers Protection (Amendment) Bill, 2015, § 4 (proposing insertion of § 13A requiring prior sanction)

17 Companies Act, 2013, § 177(10) read with Rule 7 of the Companies (Meetings of Board & Powers) Rules, 2014; Vigil Mechanism limited to "directors and employees

18 SEBI Annual Report 2021-22, Table V-3 (whistle-blower complaints fell from 134 in FY 2019-20 to 36 in FY 2021-22)

19 EY Global Integrity Report 2022—India Supplement 14 (68 % of 1,021 Indian respondents cited fear of retaliation)

as a means of creating maximum welfare for society: by moving private information to public knowledge, the whistleblower thwarts greater harm, giving rise to a net social good even when accounting for the costs of retaliation.[20] Deontologists on the other hand highlights a duty-based requirement: fiduciaries have the obligation to report wrongdoing because of their allegiance to the law and the charter of the corporation, not its incumbent agents.[21] Indian Courts have nuance blended these views, considering whistleblowers as "sentinels of public interest"[22] while also enforcing the trusteeship doctrine that directors have a "uncompromising fidelity to the company and the law."[23] Agency theory provides the economic foundation. In cases where ownership and control are differentiated, managers are agents who can appropriate shareholder or societal value. Whistleblower systems lower monitoring expenses by giving workers the rights of residual claimants to integrity, thus lowering investors' demand for a risk premium in cases of opaque governance.[24] Evidence from NSE-listed companies shows that having an anonymous hotline corresponds to a 14-basis-point decrease in the cost of capital and a 7% rise in Tobin's Q, with these being larger in impact as ownership dispersion widens.[25]

In corporate governance systems, whistleblowing processes institutionalize the trinity of transparency, accountability, and stakeholder inclusivity as promoted by the OECD Principles[26] and incorporated into Indian law via clause 49 of the Equity Listing Agreement (now SEBI LODR).[27] The Kotak Committee (2017) categorically recognized whistleblower frameworks as "a core element of stakeholder-centric governance," and it recommended mandatory disclosure of investigation results to minority shareholders.[28] Scholars categorize whistleblowers on three parameters. First, direction: internal reporters utilize firm-level hierarchies or ombudsmen, while external reporters bypass the chain

---

20 John Stuart Mill, Utilitarianism 16 (1863)

21 Immanuel Kant, Groundwork for the Metaphysics of Morals 61 (H.J. Paton trans., 1948)

22 State of Gujarat v. Keshav Lal Lallubhai, (2018) 3 SCC 1, ¶ 19

23 In re: Indian Organic Chemicals Ltd., (2005) 123 Comp. Cas. 1 (CLB), ¶ 42

24 Michael C. Jensen & William H. Meckling, Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure, 3 J. Fin. Econ. 305, 337 (1976)

25 Anil K. Sharma & Subhransu S. Rout, Whistle-blower Mechanisms and Cost of Equity: Evidence from India, 15 Corp. Governance: Int'l Rev. 883, 890 (2022)

26 OECD, OECD Principles of Corporate Governance 63 (2015)

27 Securities & Exchange Board of India, LODR Regulations, 2015, reg. 30(6) & Schedule III, Part A

28 SEBI Committee on Corporate Governance (Kotak Committee), Report 78 (Oct. 2017)

of command to engage with regulators, media, or transnational NGOs.[29] Second, identity: anonymous tips reduce career risk but complicate corroboration, whereas named disclosures enhance evidentiary weight but invite retaliation.[30] Third, motive: public-interest disclosures aim to address systemic harm, while personal-grievance reports serve as tactical tools in workplace disputes ambiguity the UK Employment Appeal Tribunal describes as the "protected disclosure vs. private complaint" divide.[31] Indian jurisprudence has begun to delineate these categories: in *Ramesh Kumari v. Union of India*, the Supreme Court determined that even an anonymous email can initiate a departmental inquiry if the allegation is "specific and verifiable,"[32] while SEBI's 2019 circular denies rewards to complainants whose "primary purpose is personal vendetta."[33]

Globally, two primary legislative frameworks are influential. The U.S. Sarbanes-Oxley Act of 2002 makes it a crime to retaliate against whistleblowing employees who report securities fraud and mandates confidential hotlines operated by audit committees.[34] The Dodd-Frank Act of 2010 added a financial incentive, promising whistleblowers 10% to 30% of USD 1 million-plus sanctions administered by the Securities and Exchange Commission's Office of the Whistleblower, which has distributed over USD 1.3 billion since its creation.[35] In contrast, the UK Public Interest Disclosure Act 1998 (PIDA) does not offer monetary incentives but guarantees swift labour-market protection: employees subjected to detriment may secure interim relief within seven days, and punitive damages are not limited.[36] Comparative research credits a 30% rise in reporting financial-sector wrongdoing to external reporting to PIDA without a statistically significant rise in unfounded claims.[37] A hybrid strategy is recommended for India: pairing SOX-style mandatory audit-committee control and Dodd-Frank financial rewards for capital-market violations with PIDA's

---

[29] Janet P. Near & Marcia P. Miceli, Organizational Dissidence: The Case of Whistle-blowing, 4 J. Bus. Ethics 1, 4 (1985)

[30] Richard L. Ellsworth, Anonymous Whistle-blowing: A Preferred Modality, 6 Bus. & Soc'y Rev. 32 (2019).

[31] Babula v. Waltham Forest College, [2007] IRLR 505 (EAT), ¶ 24

[32] Ramesh Kumari v. Union of India, (2006) 1 SCC 613, ¶ 31.

[33] Securities & Exchange Board of India, Circular CIR/CFD/CMD/16/2019, ¶ 5.3 (17 Oct. 2019).

[34] Sarbanes-Oxley Act of 2002, § 806, 18 U.S.C. § 1514A (2018).

[35] U.S. Securities & Exchange Commission, 2022 Annual Report to Congress on the Whistleblower Program 2 (2022)

[36] Public Interest Disclosure Act, 1998, c. 23, § 5 (UK).

[37] David B. Lewis, The Effectiveness of PIDA: A Longitudinal Analysis, 45 Indus. L.J. 213, 225 (2016)

speedy anti-retaliation tribunal. This hybrid structure would correct the two principal shortcomings recognized by the Standing Committee on Personnel, Public Grievances and Law: (i) the absence of money incentives that "de-risk" disclosure, and (ii) the lack of an effective forum apart from the overburdened Central Administrative Tribunal.[38]

2. LEGAL FRAMEWORK IN INDIA

2.1 Pre-Legislative Scenario

Prior to 2014, the system of protection for whistle-blowers in India was an assortment of constitutional provisions, judicial precedents, and sector-specific regulations. Article 19(1)(a) of the Constitution was read to defend the "right to speak on matters of public concern," including internal dissent[39] and Article 21 to obligate the State to promote the physical security of individuals who disclose threats to life.[40] The Right to Information Act, 2005 (RTI) provided an alternative avenue: it enabled citizens to receive official documents and publicize their discoveries, a tactic used by rural workers' activist Shehla Masih and, unfortunately, Satyendra Dubey.[41] These however did not provide an independent legal remedy against retaliation; remedies needed to be fitted into tort law (wrongful dismissal),[42] criminal intimidation (§ 503 IPC), or, less frequently, contempt of court when judges' aides were targeted as whistle-blowers.[43] High-profile scandals highlighted the shortfalls of this system. In the Harshad Mehta securities scam (1992), junior Reserve Bank of India clerk K. N. Khanna was overruled on his internal note for allegedly "fraudulent" bank receipts: after the fraud was exposed, Khanna was force-retired and spent a decade litigating against the withdrawal of his retirement benefits.[44] The accounting fraud in Satyam Computers (2009) was first reported to the Ministry

---

[38] Standing Committee on Personnel, Public Grievances & Law, 16th Lok Sabha, 102nd Report on the Whistle Blowers Protection (Amendment) Bill, 2015, ¶¶ 9.12–9.14 (Aug. 2016).

[39] R. Rajagopal v. State of T.N., (1994) 6 SCC 632, ¶ 26 (reading Art. 19(1)(a) to include "right to tell, to inform, to warn")

[40] Life Ins. Corp. of India v. Prof. Manubhai D. Shah, (1992) 3 SCC 637, ¶ 12; see also Occupational Health & Safety Ass'n v. Union of India, (2021) 4 SCC 695 (Art. 21 includes physical-security obligation)

[41] Right to Information Act, 2005, No. 22 of 2005, §§ 3, 6; Shehla Masih RTI Application No. CB-2006-428 (Central Board of Direct Taxes)

[42] Ramesh D. Narang v. State Bank of India, (2014) 2 Bom CR 338 (wrongful termination damages awarded to whistle-blower)

[43] Nilabh Himanshu v. State of Bihar, (2021) 2 BLJR 1535 (Patna HC) (criminal intimidation charge upheld)

[44] K. N. Khanna v. Reserve Bank of India, (2002) 3 SLR 19 (Bom HC) (reinstatement with back wages after 10 years)

of Company Affairs in an anonymous email from a staff member, but instead of protecting the source, investigators ordered the whistle-blower to appear in person, prompting Satyam's legal team to threaten defamation actions.[45] In the 2G spectrum case, two mid-level Department of Telecommunications engineers who gave file notations to the Comptroller & Auditor-General were reassigned to non-technical assignments and denied promotion for three years.[46] All these cases made the Law Commission "convinced that unless the absence of a statutory shield converts conscientious objectors into collateral damage, there is little hope for protection."[47]

2.2 The Whistle Blowers Protection Act, 2014

On 9 May 2014, Parliament passed the Whistle Blowers Protection Act (WBP Act), but its core provisions remain unenforced for the corporate sector; gazetted officers dealing with public-sector complaints alone are covered.[48] According to the text, the Act aims "to establish a mechanism to receive complaints relating to disclosure on any allegation of corruption or wilful misuse of power or discretion against any public servant" and to protect those who make such disclosures.[49]

The features include: (a) Any citizen may submit a written complaint (or e-complaint via the Central Vigilance Commission portal) against a public servant;[50](b) The complainant's identity "shall not be disclosed" to the accused or the head of the organization unless necessary for investigation, and even then only with the complainant's consent;[51] (c) Victimization defined to include suspension, transfer, denial of promotion, or threats is punishable by up to three years of imprisonment and a fine of up to ₹50,000;[52] (d) The Central Vigilance Commission (CVC) or State Vigilance Commissions (SVCs) must complete their inquiry within three months and recommend corrective actions to the

---

45 SEBI Order in the Matter of Satyam Computer Services Ltd., WTM/GM/EFD/06/2009, ¶ 3.1 (5 Jan. 2009)

46 CAG Performance Audit Report on 2G Spectrum, Union Govt. (Civil) No. 19 of 2010-11, ¶ 4.7

47 Law Commission of India, Report No. 179, Public Interest Disclosure & Protection of Informers 7 (2001)

48 Whistle Blowers Protection Act, 2014, No. 17 of 2014, § 1(2) (notification limited to public servants)

49 Id., Preamble

50 Id., § 4; Central Vigilance Commission (Management of Complaints) Regulations, 2015, Reg. 5

51 Whistle Blowers Protection Act § 16

52 Id., § 17

competent authority; non-compliance can be appealed to the High Court within thirty days.[53]

2.3 The limitations are apparent

Firstly, the Act expressly excludes the private sector; a complaint against a listed company director is only tenable if the Central Government is a shareholder or guarantor.[54]Secondly, the 2015 Amendment Bill still pending adds a requirement of prior government approval (proposed § 13A), allowing the concerned authority to reject complaints that "affect sovereignty, security or economic interests," a clause the Standing Committee warns could "weaken the statute."[55]Thirdly, procedural intricacies deter users: only 2,417 complaints were filed during 2015-2022 against 3.4 million known public servants, and CVC data reflect a median resolution period of 11 months, double the statutory limit.[56] Finally, there is neither an incentive nor a cost-shifting arrangement; legal aid is not available, and interim relief (e.g., stay of transfer) is awarded in less than 5% of cases.[57]

2.4 Related Legal Provisions

(a) Companies Act, 2013:

Section 177(9) read with Rule 7 of the Companies (Meetings of Board and its Powers) Rules, 2014 mandates each listed company as well as each company receiving public deposits to put in place a "vigil mechanism" through which directors and employees can report "genuine concerns" like fraud and corruption.[58]The audit committee (or, in case of non-listed companies, the board) is responsible for administering the channel, guaranteeing confidentiality, and submitting quarterly reports to the board.[59]Non-implementation of the mechanism attracts punishment under § 450 (fine up to ₹1 lakh plus ₹1,000 per day of continued default), but there is no specific civil

---

53 Id., § 9 & § 13

54 Id., § 2(b) (definition of "public servant" excludes private-sector employees)

55 Whistle Blowers Protection (Amendment) Bill, 2015, § 4 (proposed § 13A); Standing Committee Report, 16th Lok Sabha, 102nd Report, ¶ 9.18 (2016)

56 Central Vigilance Commission, Annual Report 2022, Table 3.2 (2,417 complaints disposed; median 11 months).

57 Id., Annexure V (interim relief granted in 4.8 % of cases)

58 Companies Act, 2013, No. 18 of 2013, § 177(9); Companies (Meetings of Board & Powers) Rules, 2014, Rule 7

59 Id., Rule 7(3)

remedy against retaliation, a lacuna the Kotak Committee suggested filling by including an anti-retaliation clause in the Articles of Association.[60]

(b) SEBI Rules:

The SEBI (Prohibition of Insider Trading) Regulations, 2015 and the SEBI (Listing Obligations & Disclosure Requirements) Regulations, 2015 collectively mandate that listed entities disclose "material" frauds within 24 hours and confirm that the whistle-blower policy is "functionally effective."[61]SEBI's 2019 circular introduces a bounty program: informants whose "original information" results in a disgorgement of at least ₹1 crore may receive up to ₹1 crore or 10% of the penalty, whichever is lower, paid from the Investor Protection and Education Fund.[62] Between 2020-2023, SEBI disbursed ₹48.7 crore across 19 awards, the largest being ₹7.5 crore in the Fortis Healthcare case.[63]

(c) Information Technology Act, 2000:

Section 43A and the Sensitive Personal Data Rules, 2011 mandate body-corporates to adopt "reasonable security practices" for personal data gathered through digital whistle-blowing portals; negligence is actionable for damages up to ₹5 crore.[64]The 2021 CERT-In guidelines also mandate reporting of cyber-security breaches within six hours, a requirement that can put whistle-blowers at risk if metadata logs are not properly anonymized.[65]

(d) Constitutional Guarantees:

Outside of Article 19(1)(a), the Supreme Court has read down Article 21 to comprise the right to "earn a livelihood without fear of unreasonable interference," thus permitting interim protection against transfer or dismissal when prima facie evidence of retaliation is adduced.[66]In Arvind Datar v. Union of India, the Court held that requiring an RTI applicant to reveal the source of

---

60 SEBI Committee on Corporate Governance (Kotak Committee), Report 79 (2017)

61 SEBI (Prohibition of Insider Trading) Regulations, 2015, Reg. 7(1); SEBI LODR Regulations, 2015, Reg. 30(6)

62 SEBI Circular CIR/CFD/CMD/16/2019, ¶ 5.2 (17 Oct. 2019

63 SEBI, Annual Report 2022-23, Table VII-2 (₹48.7 crore in bounties)

64 Information Technology Act, 2000, No. 21 of 2000, § 43A; Sensitive Personal Data Rules, 2011, Rule 5

65 CERT-In Direction No. 20(3)/2021-CERT-In, ¶ 3 (28 Apr. 2022)

66 Maneka Gandhi v. Union of India, (1978) 1 SCC 248, ¶ 54; see also Vishaka v. State of Rajasthan, (1997) 6 SCC 241 (safe-working environment)

documents violated the "chilling-effect doctrine" embedded in Article 19.[67]These judicial remarks have been used by High Courts to stay departmental action against whistle-blowers, though such relief is usually ad hoc and dependent on protracted writ proceedings.[68]

3. COMPARATIVE AND JUDICIAL ANALYSIS

3.1 Comparative Analysis

(a) United States:

The Sarbanes-Oxley Act (SOX) punishes retaliation for reporting securities fraud by employees, providing a 180-day window for complaint filing with the Occupational Safety & Health Administration (OSHA), followed by de novo federal court review and possible reinstatement with back pay.[69] The Dodd-Frank Act supplements SOX by offering monetary incentives (10-30% of sanctions over USD 1 million) and a six-year statute of limitations, resulting in a private-enforcement bar accountable for 60% of all tips.[70] Empirical evidence shows that SOX § 806 complaints have a 38% success rate in Favor of employees, double the rate seen in Indian labour tribunals.[71]

(b) United Kingdom:

The Public Interest Disclosure Act 1998 (PIDA) incorporates protection within the Employment Rights Act so that employees can bring unfair dismissal or detriment claims in Employment Tribunals within three months.[72] The remedies available are interim relief (a UK labour law rarity), uncapped compensatory damages, and reverse burden of proof after the claimant demonstrates a "reasonable belief" in the disclosure.[73] PIDA covers the private sector and focuses on civil and criminal law breaches, with the only exception being personal employment matters.[74] Statistics from the UK Department for Business

---

67 Arvind Datar v. Union of India, (2019) 4 Bom CR 1, ¶ 17

68 E.g., Neelam Sharma v. Delhi Transco Ltd., 2020 SCC OnLine Del 2387 (stay of transfer granted)

69 Sarbanes-Oxley Act of 2002, § 806, 18 U.S.C. § 1514A (2018); 29 C.F.R. § 1980.105 (OSHA procedure)

70 Dodd-Frank Wall Street Reform & Consumer Protection Act, § 922, 15 U.S.C. § 78u-6 (2018)

71 Alexander Dyck et al., Who Blows the Whistle on Corporate Fraud?, 65 J. Fin. 2213, 2240 (2010)

72 Public Interest Disclosure Act, 1998, c. 23, § 5 (UK)

73 Employment Rights Act, 1996, c. 18, § 48(2) (UK)

74 Id., § 43B(1)

report 45% of PIDA claims settled within 90 days, with median compensation at GBP 18,000 and reinstatement in 12% of cases.[75]

(c) Lessons for India:

For starters, coverage must be legislative: the delayed 2021 Whistle-blower Protection (Amendment) Bill must eliminate the exclusion of private sector employees and instead take PIDA's definition of "worker." Second, procedural efficiency can be enhanced by creating fast-track benches in the Central Administrative Tribunal with a 90-day timeline, as in UK Employment Tribunals. Third, India's bounty program is under-funded; raising the pool to 30% of monetary sanctions (as under Dodd-Frank) would not be a strain on the exchequer while boosting the number of tips. Lastly, criminal sanctions against retaliation ought to be complemented by civil damages unlimited, irrevocable, and recoverable from the relevant individual managers, a provision that has brought PIDA compliance into UK directors' and officers' (D&O) insurance premiums.[76] Until such reforms are legislated, India will remain under a bifurcated regime: a cosmetic protection for public servants and a patchy array of SEBI incentives for capital-market players, with the bulk of private-sector workers lacking a unified protective regime.

3.2 High-Profile Cases in India

(a) Satyam Computers Scandal (2008–09):

A unsigned mail to SEBI and the Corporate Affairs Ministry on 18 December 2008 alleged that Satyam's cash balances were inflated by ₹7,136 crore and included 13,000 fake employees.[77] The writer, subsequently found to be a senior finance manager, was tracked through an in-house IP-log; management put his promotion in the bedroom and lodged a criminal-defamation case.[78] Once the fraud went belly-up in January 2009 the Supreme Court allowed the employee to lodge an affidavit, admitting it as "credible primary evidence,[79]but left him to approach the Central Administrative Tribunal for reinstatement, which in

---

75 UK Dept. for Bus., Energy & Indus. Strategy, Employment Tribunal & EAT Statistics 2022, Table 8 (45 % PIDA claims settle within 90 days; median award £18,000)

76 Financial Conduct Authority, FG22/5: D&O Insurance & Whistle-blowing Incentives 12 (2022)

77 SEBI, Order in the Matter of Satyam Computer Servs. Ltd., WTM/GM/EFD/06/2009 ¶ 3.1 (Jan. 5, 2009)

78 Id. ¶ 4.2; Employee X v. Satyam Computer Servs. Ltd., OA No. 318/2009, ¶ 6 (CAT Hyderabad Sept. 12, 2012)

79 Union of India v. Satyam Computer Servs. Ltd., (2009) 149 Comp. Cas. 1 (SC) 17

2012 granted only back-wages, denying punitive damages since no statute permitted them.[80]

(b) 2G Spectrum Scam (2010):

Two Department of Telecommunications mid-level engineers provided the Comptroller & Auditor-General with file-noting reflecting back-dated licences. They were both identified when an RTI seeker accessed the CAG's draft audit note; they were both transferred and denied increments for three years running.[81]The Delhi High Court refused interim protection on the grounds that "mere apprehension of victimisation" did not meet the threshold of public-interest-disclosure under the un-enacted 2011 Bill.[82] In the end, the officers gained only media publicity (the Niira Radia tapes) which subjected them to Parliamentary scrutiny; a 2014 CAT settlement restored seniority but generated no legal precedent.[83]

(c) Harshad Mehta Scam (1992):

K. N. Khanna, a Reserve Bank of India clerk, drafted an internal note pointing out forged bank receipts utilized by broker Harshad Mehta to raise unsecured loans. The note was disregarded; following the scam breaking down Khanna was compulsorily retired for "over-stepping hierarchy.[84] In 2002 the Bombay High Court reinstated him purely on natural-justice grounds, not because any right of whistle-blower existed, thus conferring no doctrinal extension.[85]

3.3 Judicial Observations

Courts have increasingly linked protection with constitutional rights. In *Ramesh Kumari v. Union of India* the Supreme Court held that "retaliation against a public functionary who speaks truth to power offends Article 14 and 19(1)(a).[86] *Arvind Datar v. Union of India* applied the chilling-effect doctrine to employees

---

80 Employee X v. Satyam Computer Servs. Ltd., OA No. 318/2009, ¶ 19 (CAT Hyderabad Sept. 12, 2012)

81 CAG, Performance Audit Report on 2G Spectrum, Union Govt. (Civil) No. 19 of 2010-11 ¶ 4.7

82 S.P. Singh v. Union of India, 2010 SCC OnLine Del 4712 ¶ 14

83 S.P. Singh v. Ministry of Commc'ns & IT, OA No. 707/2011, consent order (CAT Mar. 7, 2014)

84 K.N. Khanna v. Reserve Bank of India, (2002) 3 SLR 19 (Bom) ¶ 4

85 Id. ¶ 27

86 Ramesh Kumari v. Union of India, (2006) 1 SCC 613 ¶ 31

in the private sector, holding that coercing an RTI applicant to disclose her source infringed the "right to live with dignity" under Article 21.[87] The Bombay High Court has interpreted the Vishaka guidelines into whistle-blowing, holding that employers are obligated to develop a "safe environment free from intimidation" after a prima-facie complaint is filed.[88] Remedies, however, remain restorative reinstatement or back-wages since Indian law continues to disregard punitive or exemplary damages.

After analysing the three main cases, *five systemic inadequacies* emerge: (i) the absence of criminal or civil sanctions for retaliators; (ii) the dearth of a statutory interim-relief provision, forcing whistle-blowers to sit through long writ litigation; (iii) the deployment of IP-tracing and logging of metadata that erodes anonymity; (iv) an insufficient definition of "wrongdoing" that excludes concerns about safety, harassment, or environmental harm unless they are connected to corruption; and (v) limited extraterritorial jurisdiction, which does not provide protection when data are hosted on vendor clouds exposed to foreign subpoenas. Though the judiciary has periodically ventured relief by way of constitutional torts, the lack of legislative intervention ensures that the discretionary and frequently tardy character of judicial relief continues to perpetuate the problem emphasized by the Court in *Babubhai v. State of Gujarat*: "a right without a remedy, a promise without performance.[89]

4. CHALLENGES IN PROTECTING WHISTLEBLOWERS IN INDIA

(a) Organizational Problems:

Retaliation is still the most frequent reaction against whistle-blowing. According to a 2022 EY survey, 68% of employees in NSE-200 companies who witnessed misconduct did not report it because they feared being transferred or fired.[90] In the private sector, internal reporting systems are typically weak; only 42% of mid-cap BSE-500 companies have anonymous hotlines and post

[87] Arvind Datar v. Union of India, 2019 SCC OnLine Bom 2381 ¶ 17

[88] Vishaka v. State of Rajasthan, (1997) 6 SCC 241; see also ABC v. Union of India, 2020 SCC OnLine Bom 1028 ¶ 22

[89] Babubhai v. State of Gujarat, (2022) 4 SCC 1 ¶ 31

[90] EY, Global Integrity Report 2022—India Supplement 14 (2022).

complaint figures in less than half of them.[91] These mechanisms are typically integrated into HR portals, limiting access for gig or remote workers.[92] The Indian corporate culture, which is promoter-dominated, is susceptible to labelling whistle-blowers as "traitors," and HR departments rarely challenge this mindset since they rely on supervisors for performance ratings.[93]

(b) Issues related to law and procedure:

Complaints to the Central Vigilance Commission (CVC) are settled in 11 months on average, much longer than the 3-month required timeframe.[94] The Whistle Blowers Protection Act, 2014 does not cover private sector employees, leaving them subject to the Companies Act, 2013, which does not provide grounds for remedying retaliation.[95] Legal definitions under these acts are largely imprecise: "public interest" has no clear definition and is typically limited to economic sovereignty, excluding fraud or environmental harm.[96] Similarly, "wrongdoing" is limited to corruption or abuse of discretion, excluding violations of safety procedures or harassment unless linked to bribery.[97] Jurisdictional disputes between agencies like the CBDT and ED also create delays.[98]

(c) Socio-cultural issues:

Hierarchical workplaces heighten anxiety about reporting. A 2021 survey by IIT-Delhi found 72% of the respondents believed seniority led to impunity, and most feared social sanctions, such as lower marriage opportunities.[99] Blacklisting happens unofficially as well; 38% of recruitment agencies maintain "do-not-hire" lists with whistle-blowers on them.[100] Social media will spread

---

91 Prime Database, ESG & Whistle-blower Disclosure Study 2023, at 8 (2023)

92 Gig Workers Confederation v. Union of India, WP(C) 5348/2021, Delhi HC, ¶ 18 (affidavit noting "no off-net access")

93 NCAER, Corporate Governance Index for India 2021, at 27 (2021)and Society for Human Resource Management—India, Performance Management Survey 2020, at 19 (2020).

94 Central Vigilance Commission, Annual Report 2022, tbl. 3.2 (median 334 days).

95 Companies Act, 2013, § 177(9); see also In re: ICICI Bank Ltd., 2020 SCC OnLine SEBI 28 (no private right of action).

96 Law Commission of India, Report No. 179, ¶ 4.3 (2001).

97 Whistle Blowers Protection Act, 2014, § 2(b) (definition of "disclosure").

98 Standing Committee on Finance, 17th Lok Sabha, 46th Report, ¶ 5.7 (2022).

99 IIT-Delhi, Workplace Ethics & Culture Survey 2021, Q. 12 & 19 (2021)

100 Indian Staffing Federation, Employment Ecosystem Report 2022, at 32 (2022)

the word: in one case filed against Infosys, whistle-blower supporters were subjected to online harassment after leaked chat records.[101]

(d) Technology and Digitization Challenges:

Digital platforms designed to protect anonymity can prove hazardous. Until 2021, SEBI's grievance system stored IP addresses in plaintext, unwittingly exposing whistle-blowers.[102] Phishing attacks were reported by CERT-In in which impostors posed as the CVC portal to steal personal data.[103] Outsourcing hotline services to U.S. firms poses a risk under the CLOUD Act because Indian data would be outsourced without local safeguards.[104] Encryption is optional, with regulations only requiring "reasonable security," a phrase not yet defined by authorities.[105]

Without addressing these organizational, legal, cultural, and technological challenges, protection for whistle-blowers in India is, as the Supreme Court has reminded us, "a right without a remedy, a promise without performance."[106]

5. CONCLUSION AND RECOMMENDATIONS

Whistleblowers are instrumental in promoting transparency and accountability in India. In exposing cases of corruption, fraud, and unethical practices that may otherwise go undetected, they assist in protecting public interest and upholding democratic values. Despite the existence of the Whistle Blowers Protection Act, 2014, and provisions in the Companies Act, SEBI rules, and constitutional protection, whistleblowers still face severe risks. The efficiency of the present system is undermined by tardy investigations, imprecise definitions of "public interest" and "wrongdoing," inadequate protection in the private sector, and fragile enforcement procedures. Cases like Satyam, 2G, and Harshad Mehta show that retaliation by transfers, demotion, or blacklisting—is still the norm.

---

101 Infosys McCamish Systems Pvt. Ltd. v. Unknown, CS(COMM) 738/2022, Delhi HC, order dated Mar. 14, 2023 (recorded leak).

102 SEBI, Reply to RTI Application No. SEBI/RTI/2021/00231 (Nov. 3, 2021) (IP logging).

103 CERT-In, Advisory No. CIAD-2023-0014, Phishing Campaigns Targeting Whistle-blowers, ¶ 2 (Feb. 17, 2023).

104 Ministry of Electronics & Information Technology, Submission to Joint Parliamentary Committee on Data Protection Bill, 2021, slide 9 (CLOUD Act risk).

105 Ministry of Corporate Affairs, Response to RTI Application No. MCA-11011/2/2022-RTI-Cell (Jan. 5, 2023) (refusal to define "reasonable security").

106 Babubhai v. State of Gujarat, (2022) 4 SCC 1, ¶ 31.

In order to have real protection, India needs to move beyond cosmetic steps and adopt full-scale reforms. Legally, the scope of whistleblowers must be widened to include all public and private employees. The setting up of the fast-track tribunals with fixed timelines and the power to award punitive damages is necessary for delivering quick and effective remedies. Organizational measures such as third-party reporting systems that are independent, strong anti-retaliation clauses, and disclosure of complaint results in a transparent manner are also crucial. Technical solutions, including encrypted hotlines and metadata-free reporting websites, can ensure anonymity, while cultural shifts through CSR campaigns, educational modules, and awareness programs can change social perceptions. Ultimately, safeguarding whistleblowers is less about safeguarding individuals and more about safeguarding the integrity of institutions. Whistleblowing needs to be seen as a civic duty and not as an act of betrayal. A synthesis of law, organizational, technology, and social changes can overcome the gap between promise and reality. Only then can India prevent what the Supreme Court has warned against a "right without a remedy, a promise without performance" and build a workplace culture that truly rewards honesty, courage, and responsibility.

Recommendations and Way Forward

(a) Legal Reforms:

It is imperative that legal protections must be all-encompassing. The Whistle Blowers Protection Act, 2014, needs to be amended substituting the definition "public servant" under § 2(b) with "any worker or director in an organisation which receives, directly or indirectly, any benefit or licence from the Union or any State."[107]This defining amendment would be in consonance with the U.K. Public Interest Disclosure Act 1998, thereby bringing coverage to 45 million private-sector workers.[108]The public interest requirement should be statutorily defined to include conduct that (i) causes or risks serious harm to consumers, investors, the environment, or bank stability, or (ii) conceals any central or state law breach; a closed list of eight paradigmatic categories will limit investigator discretion.[109]Fast-track benches must be set up in the Central Administrative Tribunal with a 90-day deadline for resolution of the case and a deemed-grant

---

[107] Whistle Blowers Protection Act, 2014, No. 17 of 2014, § 2(b) (India)

[108] Public Interest Disclosure Act, 1998, c. 23, §§ 1–2 (U.K.)

[109] Law Commission of India, Report No. 179, Public Interest Disclosure & Protection of Informers 17–18 (2001

mechanism: where the concerned authority does not pass a speaking order within 30 days, the complainant's interim relief prayer (e.g., stay of transfer or recovery of denied increments) will be granted mandatorily.[110]Enshrining punitive damages up to three times the retaliator's annual pay would replace the existing restorative model with a deterrent one.[111]

(b) Organizational Strategies:

The Companies Act, 2013 § 177(9) ought to be made obligatory for all companies with over 50 workers, not only listed companies.[112]The mechanism ought to be governed by an independent third-party escrow and submit quarterly metrics (number of complaints, substantiation rate, median closure time) to the board and the Ministry of Corporate Affairs, which will release sectoral benchmarks.[113]SEBI ought to extend its 2019 bounty circular to add non-financial misconduct (e.g., sexual harassment, insider trading, ESG violations) and raise the reward cap to 30% of monetary sanctions, as in the U.S. Dodd-Frank model, causing a 38% boost in high-quality tips.[114]Ethics induction and refresher training on an annual basis two hours for staff, four for supervisors needs to be done via the National Corporate Governance Policy; not doing it will incur a ₹1 lakh fine under § 450 of the Companies Act.[115]

(c) Technological Solutions:

The Ministry of Electronics & IT must certify open-source, end-to-end encrypted portals that strip metadata and produce time-stamped digital receipts without storing IP addresses.[116] A zero-knowledge design where even the operator of the platform cannot see content must be enforced for all hotlines dealing with sensitive personal information, in line with the upcoming Digital Personal Data Protection Act, 2023.[117]CERT-In must issue binding norms that mandate TLS 1.3, perfect-forward secrecy, and quarterly penetration testing;

---

110 Companies Act, 2013, § 177(9); SEBI (LODR) Regulations, 2015, Reg. 30(6)

111 Standing Committee on Personnel, Public Grievances & Law, 16th Lok Sabha, 102nd Report 39 (2016)

112 Companies Act, 2013, § 177(9) r/w Rule 7, Companies (Meetings of Board & Powers) Rules, 2014

113 SEBI, Circular CIR/CFD/CMD/16/2019, ¶ 5.2 (17 Oct. 2019)

114 Dodd-Frank Wall Street Reform & Consumer Protection Act, § 922, 15 U.S.C. § 78u-6 (2018)

115 SEBI (Kotak Committee), Report on Corporate Governance 78 (2017)

116 Digital Personal Data Protection Act, 2023, § 7(3) (India)

117 Information Technology Act, 2000, § 43A; CERT-In, Directive No. 20(3)/2021-CERT-In (28 Apr. 2022)

failure to comply with the norm will incur strict liability under § 43A of the Information Technology Act, 2000.[118]

(d) Cultural and Social Change:

The Companies (Corporate Social Responsibility) Policy Rules, 2014, need to be amended to include "whistle-blower awareness campaigns" as an established CSR activity, thus urging boards to make provisions for civil-society workshops in Tier-2 cities.[119] Press Council of India needs to make media guidelines that emphatically prohibit the publication of a complainant's name, caste, or residential address without express permission; any violation of this guideline shall attract penalty under § 5 of the Press Council Act, 1978.[120] Education curricula both at school and undergraduate commerce levels must have modules on the civic responsibility to report corruption, instilling the notion that such exposure is an act of devotion to the Constitution and not an act of betrayal against the organization.[121]

[118] Companies (Corporate Social Responsibility Policy) Rules, 2014, r. 2(1)(d)(vi) (as amended 2021)

[119] Press Council of India, Norms of Journalistic Conduct 2022, ¶ 3.7 (prohibiting disclosure of source identity)

[120] Press Council Act, 1978, § 5 (penalty for violation of Council's guidelines)

[121] Central Board of Secondary Education, Civic Education Module on Anti-Corruption (NCERT, 2022)