THE THIRD PARTY NOBODY NAMED: WHISTLEBLOWER PROTECTION GAPS IN INDIA'S DATA BREACH REGIME

Abhijna Satrasala, BBA LL.B. (Hons.), Symbiosis Law School, Pune

ABSTRACT

India's DPDP Act says companies must report data breaches within 72 hours. It says nothing about the employee who finds the breach and makes the report possible. This paper asks: is that employee protected? Does it matter if they report internally to the Audit Committee under Section 177 of the Companies Act or if they go outside to the Data Protection Board? The answer is concerning. Internal protection only exists if a company treats data breaches as violations a question no Indian court has ever answered. External protection does not exist at all: the DPDP Act has no retaliation rules of its own. Looking at the EU's Whistleblower Directive, the US laws like Sarbanes-Oxley and Dodd-Frank, and even SEBI's informant system, this paper shows that India already has the tools to fix this. It just has not used them for data protection yet. If this gap stays, it does not just hurt one employee — it weakens the enforcement model of the DPDP Act, because that model depends on someone inside the company being brave enough to speak up.

I. Introduction

India's Digital Personal Data Protection Act, 2023 (the "DPDP Act"), along with the rules introduced in 2025,[1] has created one of the strictest data protection systems in the country. If a company experiences a personal data breach, it is supposed to notify both the Data Protection Board of India and every person affected, and submit a detailed report within 72 hours of becoming aware of the breach. The Act uses specific terms for the people involved in this process, and these words matter because they shape how we understand the relationship. The person whose data is involved say, someone filling out a form for a bank, hospital, or app is called the **Data Principal**. On the other side is the organisation, whether a bank, hospital, or company, that handles that data. The Act calls this party the Data Fiduciary. In law, a fiduciary is someone who is trusted to take care of something valuable for someone else, like a trustee managing a trust or a doctor caring for a patient. By calling companies **"Data Fiduciaries,"** the law quietly but clearly says: once you hand over your data, the company does not own it completely. They hold it on trust and must protect it honestly and carefully. This obligation places the Data Fiduciary under a direct duty to notify the relevant regulator and affected individuals of any breach. But the Act does not talk about the person who usually finds out about breaches first: the employee inside the company. Usually, it is not the company as a whole that notices a problem it is a compliance officer finding a mistake, or a junior staff member discovering a data leak. This employee is neither the Data Principal nor the Data Fiduciary. They are a third, unnamed figure standing between the two, faced with the choice to speak up or stay quiet. India's corporate law already has a tool for this kind of internal reporting, but it was not made with data protection in mind. Section 177(9)–(10) of the Companies Act, 2013,[2] requires certain companies like those listed on stock exchanges or heavily financed by public deposits to set up a Vigil Mechanism. Simply put, this is a safe, formal channel for employees to report concerns about fraud, unethical behaviour, or breaches of company rules to the company's Audit Committee, a small group of board members who oversee ethics and finances. Importantly, the law also protects these employees from being punished for speaking up.

On paper, these two laws seem to fit together: one demands reporting breaches, the other protects those who report wrongdoing. But in reality, they were made years apart, in different

[1]The Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
[2]The Companies Act, No. 18 of 2013, § 177 (India).

contexts, and they do not reference each other. Section 177 was created for financial fraud and ethics issues before data protection became a major issue. The DPDP Act focuses on notifying regulators but never thought about the employee who makes that notification possible. This leaves a gap: an employee who reports a data breach internally may or may not be protected by the Vigil Mechanism, depending on whether a data breach counts as a violation of the company's code of conduct a question neither law answers clearly. And if that employee reports the breach directly to the Data Protection Board, bypassing internal channels, there is no legal protection at all, because the DPDP Act does not include any whistleblower or anti-retaliation rules. This gap has mostly been ignored. Discussions about Section 177 treat it only as a tool for corporate governance and financial fraud, not data protection. And discussions about the DPDP breach rules see them only as company obligations, without considering the employee who triggers those rules. The two areas do not connect, and the employee caught in the middle remains invisible under the law.

II. Research Question

This paper asks: Does the Vigil Mechanism under Section 177 protect an employee who reports a data breach, whether inside the company to the Audit Committee, or outside to the Data Protection Board? If not, what does this mean for enforcing the DPDP Act, and how can this gap be fixed?

To answer this, the paper looks at three questions in order:

1. Does reporting a data breach internally count as a “genuine concern” or a “code of conduct violation” under Section 177 and its rules?

2. What protection does an employee have if they report a breach directly to the Data Protection Board, skipping internal channels?

3. How do other legal systems, especially the European Union with its Whistleblower Directive, handle this issue? What lessons can India learn from them?

This paper argues that this is not a minor legal detail but a serious mismatch between two laws. The DPDP Act depends on employees reporting issues to work properly, but the protection laws were not designed to support that kind of reporting.

III. Legal Framework

A. Section 177 of the Companies Act, 2013

Section 177 is part of the Companies Act[3] that governs how company boards are run. The key parts for this paper are subsections (9) and (10). Subsection (9) says that every listed company, and some other companies defined by rules, should set up a vigil mechanism — a system where directors and employees can raise genuine concerns. Subsection (10) says this system must protect those who use it from being victimised, and in special cases, people can even report directly to the chairperson of the Audit Committee. The "other companies" referred to are listed in Rule 7 of the 2014 Rules. These include companies that accept public deposits or borrow over fifty crore rupees from banks or public financial institutions. If a company is required to have an Audit Committee, that committee oversees the vigil mechanism; if not, the Board must designate a director to perform that role.[4]

But the protection Section 177[5] offers is narrower than it first appears. The concern raised must be a "genuine concern" about one of three things: unethical behaviour, suspected or actual fraud, or a violation of the company's code of conduct or ethics policy. Nowhere in Section 177, the 2014 Rules, or SEBI's regulations do these categories expressly include data protection, cybersecurity, or a failure to report breaches as required by law. The vigil mechanism was designed to catch financial and ethical wrongdoing the words "fraud" and "code of conduct" make this clear. This is an important point: whether a data breach counts as something reportable under Section 177 is not clear from the statute itself. It depends on how a court, the Audit Committee, or the company's whistleblower policy interprets "code of conduct or ethics policy." If a company includes data protection in its code, a breach might be reportable. But many companies treat data protection as a separate matter, so employees reporting breaches could fall outside the vigil mechanism's protection.[6]

B. The Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025

The DPDP Act imposes a different kind of duty. Section 8(6)[7] requires every Data Fiduciary to notify the Data Protection Board and each affected Data Principal when a personal data

[3]The Companies Act, No. 18 of 2013, § 177 (India).
[4]Anil Kumar & Seema Gupta, Decoding Whistle Blowing Policies of Indian Companies, ICSI CHARTERED SECRETARY, Dec. 2023, at 76.
[5]The Companies Act, No. 18 of 2013, § 177 (India).
[6]Samruddhi Varma, Understanding Whistleblowing Practices and Regulations in India's Corporate Sector: A Focus on Section 177 of the Companies Act, 6(2) INT'L J.L. MGMT. & HUMANITIES 805 (2023).
[7]The Digital Personal Data Protection Act, No. 22 of 2023, § 8(6) (India).

breach occurs. Rule 7 of the DPDP Rules elaborates on this: first, an immediate notice to the Board describing the breach, followed by a full report within 72 hours explaining what caused it, what was done to fix it, who is responsible, and how to prevent it in future. Rule 6 further requires Data Fiduciaries to maintain reasonable security safeguards to prevent breaches before they happen.[8] However, neither Section 8 nor the Rules make any reference to the employee's role. The duty is on the organisation, owed to the regulator and the individuals whose data was affected. The law does not address how the organisation discovers breaches, nor does it protect the person who reports one.[9] This matters because, in practice, organisations rarely discover breaches through automated systems. Usually, an employee in IT, compliance, or another department — notices something wrong and speaks up.[10] The entire enforcement system of the DPDP Act depends on that person coming forward, yet offers them no protection whatsoever.[11]

C. The Comparators Already Built into Indian and EU Law

Two existing frameworks show that Indian law is capable of filling this kind of gap when it chooses to. SEBI's informant system under the PIT Regulations, 2015 allows anyone employees or others to report insider trading directly to SEBI using a Voluntary Information Disclosure Form.[12] It guarantees confidentiality and, in some cases, monetary rewards. This is a fully external reporting channel focused on one type of wrongdoing, with protections that do not require internal reporting first.[13] The EU's Directive 2019/1937 goes further in precisely the area under study here: it explicitly includes breaches of EU data protection law, such as the GDPR, as protected whistleblower concerns.[14] It requires Member States to establish both internal and external reporting channels, with full protection from retaliation, all within a single coherent system. Both examples illustrate the same point from different angles. Indian law already has an external whistleblower system tied to a regulatory duty, in SEBI's case. EU law has linked data protection breach reporting directly to whistleblower protection by design. But neither model has been applied to the DPDP Act. The tools exist within Indian and comparative

[8]Digital Personal Data Protection Rules, 2025, r. 6, r. 7 (India).
[9]Rupin Chopra & Apalka Bareja, Fraud Reporting under Companies Act vis-à-vis Whistleblower Mechanism, S.S. RANA & CO. (Apr. 19, 2024).
[10]Praveen Yadav & Rajesh Yadav, Privacy in the Digital Age: A Critical Study of the DPDP Act 2023 and its Implications, 3(2) RSCH. COMMC'NS 32 (2025).
[11]Data, Control, and Power: Decoding India's Digital Personal Data Protection Act, 2023, 6(4) GLOBAL PRIVACY L. REV. (2026) [GPLR2026002].
[12]Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015, Regulation 22 (India).
[13]SEBI Notifies Informant Mechanism/Informant Reward Policy under PIT Regulations, SHARDUL AMARCHAND MANGALDAS (Sept. 23, 2019).
[14]Council Directive 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 O.J. (L 305) 17.

law; they simply have not been connected to this particular issue yet.[15]

IV. Core Analysis

A. Does an Internally Reported Data Breach Fall Within Section 177?

Section 177(9) and Rule 7 protect reports concerning "unethical behaviour, actual or suspected fraud, or violation of the company's code of conduct or ethics policy."[16] A data breach does not neatly fit any of these categories as the legislature likely envisioned them. It is not necessarily fraud — breaches can occur due to mistakes or technical flaws, not dishonesty. It is not automatically unethical behaviour, unless someone deliberately neglected their duties or attempted to conceal something. That leaves only one option: a breach might count as a "violation of the company's code of conduct or ethics policy." But whether that is true depends on whether the company's code includes data protection or information security. This is not a minor detail. Many companies confine their code of conduct to matters such as bribery or conflicts of interest, treating data protection policies as separate rules managed by IT. If that is the case, an employee reporting a breach is, technically, reporting something the vigil mechanism was never designed to cover, and the protection Section 177 promises may not apply. One might argue that courts or Audit Committees will read "ethics policy" broadly and treat the mishandling of personal data as an ethical failure. That is plausible, but it remains speculative no Indian court or regulator has ruled on the question, since these rules are still new. Employees today face genuine uncertainty, and research on whistleblowing shows that when people are unsure whether they will be protected, they are just as likely to stay silent as if no protection existed at all.[17]

B. What Protects the Employee Who Reports Externally?

Section 177[18] offers no protection here, because it covers only internal reporting. The DPDP Act, for its part, contains no whistleblower or anti-retaliation rules to protect employees who report externally no promise of confidentiality, no shield against retaliation, no safe channel to raise concerns outside the company. This is the most significant gap. Precisely where protection

[15]Rüdiger Harms, Patrick Gerardy & Johannes Natus, New EU Directive Strengthens Protection of Whistleblowers, CLEARY GOTTLIEB STEEN & HAMILTON, Alert Memorandum (Oct. 22, 2019).
[16]The Companies Act, No. 18 of 2013, § 177(9)–(10) (India).
[17]Jeannette Taylor, Internal Whistle-Blowing in the Public Service: A Matter of Trust, 78 PUB. ADMIN. REV. 717 (2018).
[18]The Companies Act, No. 18 of 2013, § 177 (India).

matters most when an employee believes the company cannot or will not handle the breach properly the law offers none. Indian law already demonstrates that this kind of protection is achievable. SEBI's informant system allows anyone to report insider trading directly to the regulator, with confidentiality and even financial rewards, without any requirement to report internally first. This shows India possesses the legal infrastructure to build strong, protected external whistleblowing channels. That the DPDP Act lacks this feature is a legislative choice, not a legal limitation.[19] The EU's Whistleblower Directive reinforces this point: it treats data protection breaches as protected whistleblower concerns, fully integrated into a single legal framework.[20]

C. Why the Gap Matters Beyond the Individual Employee

This is not merely a question of fairness to whistleblowers, though that matters too.[21] The gap also weakens the entire enforcement architecture of the DPDP Act. The 72-hour reporting clock begins only once the company "becomes aware" of a breach, and awareness usually begins with an employee. If that employee fears retaliation or faces legal uncertainty, they may stay silent, delaying both the clock and the company's response. Further, the DPDP Act imposes only financial penalties, not criminal ones — which makes honest, timely internal reporting even more critical, since regulators cannot rely on criminal investigation to uncover concealed breaches.[22] A law that depends so heavily on voluntary reporting, yet offers no protection to the reporter, undermines its own objectives.

D. What This Analysis Establishes

Viewed together, internal and external reporting reveal one continuous gap. Internally, protection exists only in theory, contingent on how companies and courts interpret vague phrases such as "code of conduct." Externally, protection simply does not exist. Both Indian law (through SEBI's example) and international law (through the EU Directive) demonstrate that this gap was avoidable. Working models already exist they have simply not been extended to data protection. This mismatch leaves a compliance system that depends on employees to

[19]Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015, ch. IIIA (India).
[20]SEBI Notifies Informant Mechanism/Informant Reward Policy under PIT Regulations, SHARDUL AMARCHAND MANGALDAS (Sept. 23, 2019).
[21]The Whistle Blowers Protection Act, No. 17 of 2014 (India).
[22]Jidesh Kumar, Data Breach Notification Obligations Under the DPDP Act & DPDP Rules: Building a Modern Incident Response Framework for Indian and Multinational Enterprises, KSANDK.COM (Nov. 19, 2025).

report problems sitting alongside a protection system that neither recognises nor supports those employees.

V. Comparative Analysis: How Other Jurisdictions Handle This Intersection

The third research question asks how other jurisdictions handle the overlap between data breach reporting and whistleblower protection. Three examples are instructive: the EU's Whistleblower Directive, the US approach under Sarbanes-Oxley and Dodd-Frank, and India's own SEBI informant system. Each resolves the problem differently, together illustrating the range of options available to India.

A. The EU Model: A Single, Clear System

The EU's approach is the most straightforward. It does not treat data protection and whistleblowing as separate concerns. The Whistleblower Directive includes data protection breaches as protected concerns, requiring Member States to establish internal and external reporting channels and to protect whistleblowers from retaliation, all within one clear framework. It even layers on the GDPR's confidentiality rules to protect whistleblowers' personal data. For India, the lesson is not that an entirely new whistleblower law is required. Instead, the connection between data breach reporting and whistleblower protection should be spelled out clearly in the DPDP Act or its rules, rather than left for courts or companies to infer.[23]

B. The US Model: Two Laws, Two Functions

The United States splits protection and incentives between two statutes. Sarbanes-Oxley[24] protects employees from retaliation when they report securities fraud, whether internally or to regulators, and permits them to sue if that protection fails. Dodd-Frank[25] adds a financial reward for employees who provide original information leading to enforcement action, even where they choose not to report internally first. This split demonstrates that protection and reward are separable policy choices. Protection against retaliation is essential and can stand alone; rewards are an optional supplement that may encourage more reporting but are not

[23]Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201, § 806.
[24]Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, 15 U.S.C. § 78.
[25]Rüdiger Harms, Patrick Gerardy & Johannes Natus, New EU Directive Strengthens Protection of Whistleblowers, CLEARY GOTTLIEB STEEN & HAMILTON, Alert Memorandum (Oct. 22, 2019).

necessary to keep whistleblowers safe.

C. The Indian Model: A Ready-Made Example

SEBI's informant mechanism is the most instructive example, precisely because it is Indian law, not a foreign import. It already provides an external reporting channel independent of companies, together with confidentiality rules and financial rewards. This demonstrates that India possesses the legal culture, technical capacity, and institutional appetite to build such systems. That the DPDP Act lacks these features is not because India cannot build them — it is because the law's drafters did not extend this existing model to data protection.[26] Considered together, these three models suggest a layered approach for India: the EU shows the need to name protected categories such as data breaches explicitly; the US shows that anti-retaliation protections can be built first and separately from reward programmes; and SEBI shows that India need not import new ideas, but can extend what it already has.[27]

VI. Judicial Treatment: Lack of Direct Precedent and What Related Cases Reveal

No Indian court has, so far, directly ruled on whether reporting a personal data breach qualifies as a "genuine concern" under Section 177(9), or as a "code of conduct" violation under Rule 7 of the 2014 Rules. This is unsurprising, given that the DPDP Rules are still new, but adjacent case law offers useful guidance. Indian courts have previously intervened where legislation was silent on whistleblower protection. In Vineet Narain v. Union of India,[28] the Supreme Court ordered statutory oversight of the CBI through the CVC, filling a legislative gap. Similarly, following the murder of NHAI engineer Satyendra Dubey, the Court directed the government to establish an interim whistleblower mechanism in 2003, which later crystallised into the Whistle Blowers Protection Act, 2014. This history shows a judiciary willing to bridge legislative gaps, and it may do so again here. That said, protection is not unconditional: in the Coal Block Allocation case, the Supreme Court held that whistleblowers acting in the public interest deserve protection, while those misusing information may face legal consequences. The Court in Common Cause v. Union of India[29] further reaffirmed the CVC's role in handling whistleblower complaints a role the Data Protection Board currently lacks under the DPDP

[26]Rüdiger Harms, Patrick Gerardy & Johannes Natus, New EU Directive Strengthens Protection of Whistleblowers, CLEARY GOTTLIEB STEEN & HAMILTON, Alert Memorandum (Oct. 22, 2019).
[27]Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201, § 806.
[28]Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015 (India).
[29]Digital Personal Data Protection Rules, 2025, r. 7 (India).

Act. Where courts have addressed Section 177(9)–(10) directly, they have adopted a narrow construction. In Registrar of Companies v. Unitech Holidays Ltd. (2024), the court held that these provisions must be interpreted strictly and literally, reinforcing the concern that phrases such as "code of conduct" may not readily extend to data breach reporting. No case has directly answered the question posed in this paper, simply because none has yet come before the courts. But existing decisions reveal a judiciary willing to fill legal gaps, a narrow reading of Section 177, and a private-sector reality in which employees, lacking clear legal protection, remain stranded across a patchwork of forums the very problem the recommendations below seek to address.

VII. Recommendations

First, and most simply, the Ministry of Electronics and Information Technology should clarify either by amending the DPDP Rules, 2025,[30] or by issuing official guidance that reporting a suspected or actual personal data breach constitutes a "genuine concern" under Section 177 and Rule 7 of the Companies (Meetings of Board and its Powers) Rules, 2014.[31] This should apply regardless of whether a company's code of conduct specifically mentions data protection. A short, unambiguous statement of this kind would remove the confusion employees currently face regarding whether they are protected when they speak up.

Second, the DPDP Act or its Rules should incorporate protections against retaliation for employees who report breaches directly to the Data Protection Board.[32] This could follow the model of SEBI's informant system under the PIT Regulations, 2015, by ensuring confidentiality, shielding whistleblowers from disciplinary or legal action arising from their report, and permitting them to bypass internal channels where necessary. As in the United States, these protections can exist independently, without requiring rewards or incentives, which may be considered separately at a later stage.

Third, the Data Protection Board itself should be given a formal role in receiving and safeguarding such reports, akin to SEBI's Voluntary Information Disclosure process. This would give employees a trusted external avenue that does not depend on their company's

[30]Jidesh Kumar, Data Breach Notification Obligations Under the DPDP Act & DPDP Rules: Building a Modern Incident Response Framework for Indian and Multinational Enterprises, KSANDK.COM (Nov. 19, 2025).
[31]Vineet Narain v. Union of India, (1998) 1 S.C.C. 226 (India).
[32]Common Cause (A Regd. Soc'y) v. Union of India, (2018) S.C.C. OnLine S.C. 682 (India).

goodwill or internal policies.

Fourth, while awaiting legislative reform, companies covered by Section 177 can act on their own initiative. They may explicitly include data protection and information security violations within their codes of conduct or ethics policies, making clear that the vigil mechanism protects employees who report breaches, and may adopt independent policies protecting employees who report breaches internally or to the Data Protection Board.

VIII. Conclusion

This paper began with what appeared to be a narrow legal question: does Section 177's Vigil Mechanism protect an employee who reports a data breach, either internally or to the Data Protection Board? The answer is concerning. Protection within companies exists largely in theory, contingent on how vague terms such as "code of conduct" are interpreted. Outside the company, no protection exists at all. This gap is not merely theoretical it threatens the effectiveness of the DPDP Act, because the 72-hour reporting clock begins only once someone inside the company becomes aware of a breach, and that awareness usually originates with an employee. Without protection, employees may remain silent, delaying reports on which the law depends. Because the DPDP Act relies on financial penalties rather than criminal sanctions, timely and honest internal reporting becomes even more essential, since regulators cannot rely on criminal investigation to uncover undisclosed breaches. The fix is not radical: other systems have already implemented it. The EU protects data breach reports as part of its whistleblowing framework. The United States shows that anti-retaliation rules and incentive programmes can be developed as separate, sequential steps. India's own SEBI informant system demonstrates that the tools and institutional culture for strong, protected external reporting already exist. What remains missing is the political and legislative decision to extend these tools to data protection, along the lines proposed above. Until that happens, employees who discover breaches will remain caught between two laws, protected by neither.