



NON-MATERIAL PRIVACY HARM IN INDIA: RETHINKING REMEDIES UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Samraat Singh¹, Dr. Ajeet Kumar²

¹Research Scholar, Faculty of Law, Major S. D. Singh University, Farrukhabad (U.P.)

²Associate Professor, Faculty of Law, Major S. D. Singh University, Farrukhabad (U.P.)

Article DOI: <https://doi.org/10.36713/epra29085>

DOI No: 10.36713/epra29085

ABSTRACT

Distress, humiliation and interference with autonomy are other concerns in relation to the protection of personal data, but they are not measurable financial concerns, which presents a remedial challenge when the unlawful processing results in such distress. This article considers whether the Digital Personal Data Protection Act, 2023 (DPDP) in India strikes the right balance between constitutional recognition of privacy and individual remedies. It uses doctrinal analysis and literature review of Indian literature, comparison of the relevant foreign judgments and descriptive analysis of the official secondary data. According to a Parliamentary reply released in March 2026, CERT-In reported and tracked a total of 2,944,248 cybersecurity incidents during 2025, which is significantly higher than 1,402,809 incidents reported during 2021. The findings of a calculated increase of 109.9 per cent ought to offer institutional context, but such observations do not necessarily at this stage provide a prevalence of compensable privacy injury. Provisions that are in force at the time of the legal analysis are distinguished from those that are to be implemented at a later time. It highlights a lack of compensation within the DPDP scheme, and the absence of constitutional, consumer and private law opportunities. Indian literature and some of the decisions made in the past, support the separation of infringement from injury, and hold that there need not be any economic injury, to give rise to emotional distress. The article advocates the independent adjudicatory process, different standard for non-material harm, proportionate disclosure of evidence, and coordinated preventive and compensatory measures. Its contribution is a framework: it isn't every security incident that is a privacy violation for which action can be taken, but it is a framework that does link the interest affected, proof of injury, and institutional capacity.

KEYWORDS: Non-Material Harm; Informational Privacy; DPDP Act; Individual Compensation; Indian Data Protection Law; Access to Remedies.

1. INTRODUCTION AND RESEARCH PROBLEM

A person whose confidential medical information is disclosed, may experience humiliation without loss of income. Another might stay fairly calm, yet lose the means of regulating the flow of personal details. These examples reveal one of the challenges for legal systems that easily accept financial loss, and require uncertain or inaccessible evidence of other injuries. Personal data protection is incomplete if it fails to address the interests covered by substantive law by any appropriate remedy. The Digital Personal Data Protection Act, 2023 (hereafter referred to DPDP Act) offer duties and enforcement mechanisms for digital personal data. That omission does hold significance since the questions that are addressed by regulatory intervention and individual reparation are distinct matters. A penalty does not have to resolve an affected person's injury; it can be used to correct an organization for poor adherence to rules. Just as well, compensation needs to be contingent - not automatic - for every procedural irregularity, but for a legally recognized injury.

The constitutional base is provided by Justice K. S. Putt swamy (Retd.) v Union of India, where privacy is placed in the context of dignity, liberty and personal autonomy.[2] The practical implications need to be looked into. Once a right is found to be a fundamental right, the forum and evidentiary standard because of which affirmative financial relief is to be provided

in each interference is not specified. Such connections would need to be taken into account in a credible remedial framework where information about the processing largely falls under the control of an organization.

2. RESEARCH OBJECTIVES AND METHODOLOGY

2.1 Objectives and Research Design

The study aims to understand four things: first, what is meant by non-material privacy injury; second, an evaluation of the DPDP framework and additional Indian remedies; third, a closer examination of the official data surrounding incidents and Indian scholarship within its sphere of influence; and fourth, to rise to the level of developing a comprehensive framework for individual redress. It is of doctrinal and normative design, aided by a descriptive secondary data analysis. The legal analysis unit is a provision, judicial proposition or remedial mechanism. The unit of observation is a calendar year, as this correlates to a number of CERT-In incidents and is not an individual claimant or victim.

2.2 Selection and Analytical Procedure

Primary s is the DPDP Act, the Rules its Rules of 2025 and the commencement notification, relevant provisions of the Information Technology Act, Consumer Protection Act and decisions by the Constitution of India. The foreign decisions



were chosen because they directly addressed issues of non-material damage, causation, loss of control, or representative procedure. The United Kingdom and Singapore are illustrative of the different outcomes that can be achieved through different statutory language, and the European Union provide an express model for compensation for such liability.

The literature search conducted is a purposive literature search. This takes into account the Indian legal scholarship on privacy and compensation, the recent legal commentary, and India-specific empirical research on privacy attitudes. The search was identified in Public scholarly web repositories, official legal portals, publisher web sites and university sites. It would be possible to include only the things that related to the interests being protected, were enforceable, or were accessible by a claimant. Legislation was compared to the dates it came into effect, and the references of commentary were assessed against the primary texts. No attempt has been made to identify all of the relevant publications or unreported judgments.

The analysis has been structured around five questions relating to law: who or what interest is protected, what conduct does it regulate, what is the nature of the injury, what forum is there to address complaints, and what relief is available. The outcome of this comparison is an assessment of doctrinal consistency and accessibility. These categories are not variables in a statistical model; nor do they represent independently validated qualitative coding. These categories are not variables in statistical model, and they do not constitute independently validated qualitative coding.

2.3 Quantitative Method and Scope

The numerical data is from a Parliamentary reply given by the Ministry of Home Affairs on 24 March 2026 on CERT-In observations from 2021 to 2025 and have been calculated by taking the ratio of the current year's observations to the previous year's observations for each corresponding period, teased by 100 to assign a percentage value. Percentages are given to 1 decimal place. No rate per internet user is estimated, and the first year is used as a baseline.

The study draws upon published information only, without carrying out any new surveys, interviews or records of claims. The results of published surveys go to the authors of the original survey. Five aggregate administrative observations would not give five behavior observations, and as such, it would not be appropriate to make inferential tests, causal estimates, or national prevalence claims. Notices under the Act come to an end on 28 September 2026. This design allows for a logical analysis of remedial architecture, and helps to leave the matter of the performance of institutions and individual rates of injury to the next round of empirical study.

3. INDIAN LITERATURE AND THE RESEARCH GAP

3.1 Constitutional and Conceptual Scholarship

The Four Parts of Privacy in India written by Bhairav Acharya reveals different legal issues relating each part of privacy the press, state surveillance, decisional autonomy, and personal information. The article has already been written prior to Putt swamy and also DPDP Act but still, it remains relevant when it comes to the understanding of why there cannot be a single formula for every financial loss to organize a privacy dispute. Its restriction for the purposes of the present inquiry is

temporal; that is: it is not interested in institutions as yet established by later legislation.

The contextual integrity approach of Nissenbaum provides an additional analytical lens. These forays on the international stage build connections between the conceptual framework and do not substitute for interpretation of Indian constitutional and statutory materials, even though they provide work to physiologically, reputational, and autonomy-based consequences.

3.2 Indian Analysis of Compensation and Enforcement

Ajay Kumar Bisht and Neeru Ganti Shanmuka Sreenivasulu analyses the DPDP Act in the backdrop of previous Indian proposals and international standards. This contribution outlines the focus of a substantive reform direction identified in their Chapter 2024 as the gap of compensation, and the support for an express entitlement for victims harmed through unlawful processing. But more detailed studies are needed to identify what may constitute non-material injury, who should bear the burden of presenting processing evidence, and how the settlement amount would differ from a regulatory fine.

In 2026, Kriti Kabra also examined the case law of exclusion of individual compensation and problems generated by the overlapping forums; her emphasis on claimant experience is welcome. The deep implication and generality of this statement that there is no meaningful remedy any longer cannot be brushed aside without looking at conditions of the means of redress, given that they are constitutional and other statutory means. Not only that, but it overlooked the expected omission of section 43A as part of the notification of the commencement, and did not consider enactment itself as the evidence that the provision no longer applies.

3.3 Empirical Evidence Concerning Indian Users

An anonymous online survey of 428 individual respondents was analyzed in Athar and colleagues' India-specific study. The 2025 manuscript, easily accessible, presents the figure of 82.2 per cent of those who claim to be aware of browsing privacy and the challenges with that awareness impacting on informed consent practice. They also examined 143 open-ended responses that link legal rights with the actual "context" of people's understanding and exercising their rights.

Care must be used when interpreting the sample. There was some use of personal contacts for recruitment and 225 of the respondents were from Uttar Pradesh. Limits generalizability expressly by the authors. The evaluation is of perceptions and reported interactions, not of injury as found in court or readiness to accept compensation. The point where it comes in is for this reason one of whether something is formally available as a complaint procedure will be graspable and usable. Its percentages do not provide any national assessments of distress.

3.4 Contribution of the Present Study

From the works surveyed, it is clear that the interests of privacy vary, and that there is a need for individual compensation, which should be put into the legislative discussion. A restatement of those parts of the proclamation would provide little more benefit. This present contribution conceptualizes this and slips them in a remedial approach



separating types of injury, access to evidence and institutional safeguards. Another important issue it discusses is a measurement issue that administrative counts of incidents indicate pressure on the system, but not how much personal injury is happening.

4. CONCEPTUAL FRAMEWORK FOR NON-MATERIAL PRIVACY HARM

If the privacy harm is not material, it is regarded here as non-material, and means an adverse impact on a personality interest that is not necessarily economic in nature. It can involve actual distress, embarrassment, damage to reputation or actual interference in informational autonomy. Not that currently there is an identical cause of action of all the categories under the Indian law. It marks out the interests that an express remedial reform should consider.

There are three concepts that should not overlap. An infringement has to do with illegal actions. An injury relates to the harmful effect of an injury on a particular interest that is protected. Risk is a potential future event. An organization can be in violation of a procedural obligation even if no actual harm comes to any individual outside of it. A breach of confidentiality on the other hand can be detrimental to the claimant's interests before they are revealed, if the disclosure occurred without permission. Anxiety about future misuse could be an actual experience and the potential for future misuse is unclear.

There's a distinct logic to emotional upset and intrusion upon autonomy as well. Distress relates to the claimant's response. Autonomy is about a diminished capacity to control a safeguarded area of life. While the absence of anxiety from a composed claimant should not contribute to a determination of exclusion, likewise, an autonomy claim should not be so general, but only exclude if the loss of control is not identified in a concrete way. Appropriate interference is where the intimate data is disclosed without consent or where it is used beyond the scope of the confidentiality after there is a valid withdrawal of consent and no alternative of authorization.

The importance of the interference is a function of the context. The difference between disclosure of the diagnosis with an authorized treating professional, to an unrelated employer. When a home address is exposed, it can be particularly impactful if there was known to be a threat. Adjudication should consider those circumstances, but not approve the prejudice that such disclosure would serve. An acknowledged injury should factor into granting relief; and a lack of psychiatric diagnosis shouldn't negate a believable distress.

This scheme of responses deals with the various elements of an incident: prevention, correction, and compensation. Preventive relief - to forestall or existing interference. There are corrective steps that can be taken for re-accuracy or for regain of practical control. Compensation refers to injuries that have happened and cannot be adequately treated in those ways. It should be based on a selection based on

reasons relevant to the claimant's situation, not a set monetary amount for each record that has been affected.

5. THE DPDP FRAMEWORK IN THE CURRENT LEGAL TRANSITION

Phase wise start has been done through Notification dated G.S.R. 843(E) on 13 November 2025. The institutional and the miscellaneous provisions in particular took effect. Section 6(9) and section 27(1)(d) (both of which relate to Consent Managers) come into effect one year after. The substantive processing obligations and individual rights and enforcement mechanisms start 18 months later. The later dates are therefore 13 November 2026 and 13 May 2027.[10]

The substantive sponsoring scheme outlined below is in force at the research cut-off, but has yet to commence. There are eighteen months in the group for which two sections are pending – 44(2) which allows for omission of section 43A of the Information Technology Act (IT Act). When assessing the present position Section 43A therefore needs to be taken into account. The impact of non-renewal on past claims will have to be separately studied and will not be possible by just looking at the date of the DPDP Act.

In the laws on the books, grievance redressal takes precedence over approaching the Board under section 13. There are powers relating to urgent mitigation, inquiry and penalties in section 27. Alternative dispute resolution (ADR) and voluntary undertakings are contemplated in Sections 31 and 32. Through these mechanisms, individual interests might be safeguarded, but none makes it explicitly clear about the general right to damages for non-material harm.

As seen in the Schedule, the difference between a sanction and a reparation is that while a reparation is binding, a sanction is not. The highest penalty for non-compliances of taking due care and caution for security measures by the definition of security in section 8(5) is INR 250 crore. The amounts mentioned in section 8(6) are only statutory limits and this amount does not mean that the quantum has been awarded or that each affected person gets it. The size of their compensation cannot prove the extent of the individual compensation in any case.

Additional provisions of the 2025 Rules pertain to safeguards, notification of breach, and exercising of rights for the individual. There are additional provisions in the 2025 Rules related to safeguarding, notification of breach, and individual's rights. However, when clarity and access is the factor, and notification in itself does not heal injury inflicted. Empowering the Board to make directions also does not solve the problem of the legal basis, its value, its limits or its enforcement of a personal damages claim.

6. QUANTITATIVE EVIDENCE AND ANALYSIS

6.1 Official Incident Series

Table 1 reproduces the five annual CERT-In counts presented in the March 2026 parliamentary reply. The describes incidents reported to and tracked by the agency. Using one published series avoids combining administrative categories or replacing complete years with partial-year observations.[3]



Table 1 Cybersecurity incidents reported to and tracked by CERT-In

Year	Recorded incidents	Change from previous year
2021	1,402,809	Not calculated
2022	1,391,457	-0.8%
2023	1,592,917	14.5%
2024	2,041,360	28.2%
2025	2,944,248	44.2%

: Ministry of Home Affairs, “Assistance to States to Tackle Cyber Incidents”, parliamentary reply published by the Press Information Bureau, 24 March 2026. Percentage changes are the author’s calculations from the reported counts.[3]

6.2 Interpretation of the Numerical Pattern

The series records a small decline in 2022 followed by three successive increases. Between 2021 and 2025, the count rose by 1,541,439 incidents, equivalent to 109.9 per cent. The largest annual increase within this period was 44.2 per cent in 2025. These calculations describe recorded administrative activity. They do not identify how much of the change arose from underlying threats, improved detection, greater reporting, or changes in the population of connected systems.

The legal relevance lies in the need for procedures capable of processing evidence and responding to incidents at scale. It does not follow that the same number of individuals suffered distress. An incident may affect many people, concern organizational systems without personal injury, or overlap with other observations. The series contains no individual-level measure of duration, severity, causation, or remedy. It therefore cannot be converted into a count of successful compensation claims.

6.3 The Measurement Gap and Its Implications

The administrative series and the reviewed user study illuminate different dimensions of the problem. Incident monitoring concerns recorded security events; privacy-attitude research concerns participants’ understanding and reported choices. Neither provides a national measure of non-material injury. Their combined value is to expose the missing connection between technical reporting, individual experience, and legal redress. Treating them as interchangeable would give an appearance of empirical precision unsupported by their design.

This gap has a concrete institutional implication. Future reporting should distinguish the number of incidents from the number of notified persons, grievances alleging particular injuries, and requests for different remedies. Published outcome data should separately identify settlements, corrective directions, compensation decisions, and unsuccessful claims. Such categories would permit assessment of access and responsiveness while avoiding an assumption that every complaint establishes a violation.

The figures also cannot evaluate the substantive DPDP regime’s deterrent effect. Most of the relevant obligations and enforcement powers had not commenced during the observed years. A claim that the Act caused, prevented, or failed to prevent the recorded increase would therefore lack an adequate legal and methodological foundation. The defensible conclusion concerns institutional preparedness and the need for better injury-related evidence.

7. EXISTING INDIAN REMEDIES AND THEIR LIMITS

Section 43A of the Information Technology Act pays compensation if a body corporate negligently fails to take reasonable security precautions regarding sensitive personal data and as a result causes wrongful loss or wrongful gain. Even in the transitional phase, these provisions are applicable and the conditions create a universal remedy for all acts that cause non-material injuries is not possible.

In suitable case, relief may be provided by constitutional proceeding. While monetary constitutional relief is possible in principle, the neutral rule set forth in *Nil Abati Behera v State of Orissa* for a proven violation of the fundamental rights in a custodial-death case would be very hard to extend to a privacy case, where issues of state responsibility, proven basic right violation, and the suitability of the proceedings would be more difficult to justify. It cannot be applied to all private data fiduciaries.

There are further options within the private law. There may also be contractual confidentiality and breach of confidentiality issues subject to qualifications regarding public records and public functions as considered in *R Rajagopal v State of Tamil Nadu*. However, disclosure of information provided by a consumer in confidence will be a violation of the Consumer Protection Act, 2019 under section 2(47)(ix) and can only be made out a claimant must prove the consumer relationship as well as the circumstances of the relief requested.

Jurisdiction remains important. The extent to which the legal effect of those civil jurisdiction restrictions in section 39 of the DPDP Act on independent compensation claim will have will be dependent on their legal basis and the judicial interpretation to be given to such a restriction. A particular independent compensation claim could be legal or not, depending on its legal basis and the nature of the judicial understanding to be afforded to such a restriction, as provided in section 39 of the DPDP Act. However, the existence of a superior-court review does not create an affordable access provision to modest individual claims, as in *Constitutional review, L Chandra Kumar v Union of India* holds that it constitutes a part of the basic structure of the Constitution.[16] Instead, the concern is diffuse and been drawn into question redress, but not wholesale elimination of all legal avenues.

8. COMPARATIVE JURISPRUDENCE ON INJURY AND PROOF

This decouples the material and non-material damage from this recognition and leaves it to the discretion of the court whether a modest infringement needs to be recognized and again renounces a minimum seriousness threshold as was done in *Österreichische Post*. It is conceptually relevant to India only



in reference to the express European entitlement which has no direct statutory parity in the DPD Act.

But, National agenesia za periodate agreed that the fear may constitute non-material damage, if the fear is justified in the circumstances. This legally relevant current effect would still need to be determined.[19] The decisions in both Quirin PrivatBank (September 2025) and the September 2025 cases also acknowledged emotional harm in the aftermath of unpermitted disclosure and the importance of showing the harmful effects and how it was caused.

In Brillon Rottler, confirmed, on 19 March 2026, that in cases involving a claim for breach of access-rights, the necessary conditions and causal damage must be established and considers possibilities of such circumstances being artificially brought about by the claimant's conduct. Simple numbers of complaints should not be used as replacement for a specific claim being deemed as abusive.

The example of the United Kingdom and Singapore illustrate the importance of statutory differences. In *Lloyd v Google*, cases of uniform damages in breach of the statutory order of the then applicable DPA did not require individual evidence of the relevant damage and the Court of Final Instance rejected the claim. In *Reed v Bellingham*, it was recognized that emotional distress was a statutory head of loss, but that even if open to a statutory claim, it had to be shown to be a significant loss individually. The appeal reversed the injunctive relief.

This is, therefore, a selective comparative lesson. India can identify distress and demand evidence for this and identify autonomous, rather than emotional needs as well as liability needs in the context of common liability instead of individual too. An Indian institution cannot independently give permission to give damages, based on foreign decisions. Their contribution is to alert legislators to the kind of choices involved on the one hand, and to remind them that not all harms must be monetary damages, and on the other, that not all non-economic harms are too speculative to be considered.

9.FINDINGS AND DISCUSSION

Results from the doctrinal research shows that there is a gap between the volume of interests protected and the specifically offered relief for individuals. There are significant enforcement provisions and monetary sanctions in the DPD scheme, but these do not respond to the claimant's separate request for reparation. This doesn't require proof that the incident has led to a compensable injury. This is a logical consequence of the look at destination of penalties in statute and lack of express damages entitlement.

The second is about the accessibility. Indian supplementary medicine might be able to treat specific injuries, but they have varying entry conditions. It cannot be inferred in each processing dispute that there is a consumer relation or state responsibility, handling of sensitive data in a negligent manner or an obligation of confidentiality. Thus, fragment is impacting the predictability of protection. In addition, evidential disclosure plays an important role as a claimant might require organizational records before determining the cause of action.

The numerical analysis is based on recorded incident activities, which are increasing after 2022, and personal injuries which are not measured. This distinction draws the boundaries of what quantitative evidence can be used for. This nonetheless bolsters the argument for the gathering of remedial

consequence data together with technical incident data. The measure of success with respect to a rights-based assessment should be to have the affected people know and understand the process; to provide the evidence needed; and to provide the relief appropriate.

There's also an issue as regards statutory cover. If a claim involves exemption processing, then examination of the exemption and any independent constitutional or other legal basis is required in the absence of which, the law making the exemption also creates a gap in coverage. Remedial reform should thus specify the duties for which it holds parties accountable and explicitly include a discussion of public and private responsibility. Otherwise, a seemingly broad entitlement might be constantly out of reach just in the conflicts where accountability is in question.

The most robust institutional concern is that litigation may falsely absorb resources that are sorely needed at the prevention end of the spectrum. Public enforcement may tackle collective organizational practices without individuals having to sue. That does not mean that that advantage doesn't assist with coordination and proportionate procedure, but it doesn't mean substantial demonstrated personal injury should rely solely on regulatory priority. A combined model should maintain efficient investigation along with individual relief as appropriate. The measurement of its effectiveness in the future must take into account both administrative costs and claimant outcomes, not necessarily more penalties or more damage claims connoting greater protection.

10.A PROPOSED FRAMEWORK FOR INDIVIDUAL REDRESS

10.1 Express Entitlement and Institutional Responsibility

Parliament should create an express entitlement to appropriate relief for injury caused by a contravention of specified data protection obligations. Earlier Indian legislative proposals show that compensation was a considered option: clause 64 of the Personal Data Protection Bill, 2019 expressly contemplated it.[24] Reform should now state the basis of responsibility, available defenses, compensable interests, and forum, rather than leave an entire damages jurisdiction to implication from general regulatory powers.

A specialized adjudicatory route is preferable in principle because recurring disputes will involve processing records and technically complex evidence. This preference depends on institutional independence, accessible procedure, reasoned decisions, and judicial supervision. Investigation and adjudication should be sufficiently separated. An injured person should not have to wait for the regulator to choose a case for a penalty before initiating an individual claim. Any evidential effect of prior regulatory findings should be specified by law and remain compatible with a fair opportunity to contest responsibility.

10.2 Differentiated Recognition of Injury

The proposed test begins with the protected interest and the unlawful processing alleged. The claimant must then identify the adverse consequence and connect it to the contravention. Distress requires a credible account of an experienced effect. An autonomy claim should identify the effective choice, confidentiality boundary, or control that was impaired. Bare statutory language should not replace factual



particulars, and proof of financial loss should not be an automatic requirement for either category.

Prospective risk requires separate treatment. A hypothetical possibility may justify preventive action where the legal conditions are met. A credible threat that produces demonstrated present distress may support compensation for that present injury. Actual disclosure can also constitute a completed interference whose consequences require assessment independently of future misuse. This differentiation avoids forcing all claimants into a single psychological category while preserving a meaningful threshold of proof.

10.3 Evidence and Procedural Fairness

An initial claim should identify the processing episode and provide reasonably available supporting material. Notifications, correspondence, contemporaneous descriptions, and evidence of changed behavior may assist. Medical evidence should be considered where relevant, but should not become mandatory for every emotional injury. Otherwise, access to treatment and the capacity to finance expert evidence could determine whether an equally credible harm is recognized.

Once a plausible connection has been established, the procedure should enable proportionate disclosure of relevant records within the organization's control. Requests might concern recipient information, processing logs, retention decisions, and containment measures. Confidentiality safeguards can protect unrelated persons and legitimate organizational interests. Unjustified withholding may support a reasoned adverse inference. This proposal improves evidential access without presuming damage from the existence of a security event.

Causation should also be tested against competing explanations. An external attack does not, by itself, establish that an organization complied with its obligations, but the occurrence of an attack is equally insufficient to prove liability. The inquiry should identify the relevant duty, its breach, and its contribution to the alleged consequence. Where several actors participate in processing, legislation should clarify responsibility and contribution between them so that evidential complexity does not become an unexplained obstacle for the claimant.

10.4 Appropriate Relief and Valuation

Relief should respond to the established consequence. Explanation and correction can restore practical agency; restrictions on processing may prevent continuing interference; and compensation can address injury that remains. A private diagnostic provider's unauthorized disclosure illustrates their interaction. Prompt containment may reduce future risk without necessarily eliminating distress already experienced. An award should explain what injury persists and why the selected remedy responds to it.

Valuation should consider duration, sensitivity in context, extent of exposure, demonstrated consequences, and mitigation. Income should not determine the inherent worth of dignity, and organizational turnover should not automatically determine compensatory damages. Turnover may inform public sanctions, whereas compensation requires reasons connected to injury. Published decisions can improve consistency; rigid monetary tariffs introduced before sufficient experience could conceal important differences between cases.

The decision should also explain how overlapping injuries have been treated. Distress and reputational impairment may arise from the same disclosure, yet their simultaneous description does not automatically justify separate full awards. Transparent reasoning should recognize distinct consequences while preventing duplicate recovery for an injury merely expressed through different legal labels.

10.5 Access and Coordination

Legislation should address limitation from reasonable discovery, the effect of pursuing preliminary grievance procedures, interim protection, execution, and appeal. Claimants should have assisted filing, accessible formats, and proportionate fees. Sensitive exhibits may require restricted access or redaction so that seeking relief does not reproduce the exposure complained of. Publicly available reasons should preserve enough detail to permit scrutiny of legal reasoning and valuation.

Collective procedures should permit common questions to be resolved together while allowing individual or appropriately grouped assessment of injury. Settlements must be informed and voluntary. Prior recovery for the same consequence should be taken into account, while a regulatory penalty should not be treated as money already received by the claimant. These changes require express legal authority where they create new entitlements or jurisdiction. Their performance should subsequently be assessed through published measures of access, resolution time, cost, and remedial outcomes.

11.LIMITATIONS AND FUTURE RESEARCH

The magnitude of non-material privacy harm and what awards will look like in the future are not able to be estimated in this study. The overall percentages of administrative cybersecurity are for a different phenomenon and the survey analyzed is not a sample representative injury study. The purposive literature review may not include relevant materials, and, comparative judgments may be made pursuant to statutory provisions that are inapplicable to Indian law. Therefore, the reform argument should be regarded as doctrinal or normative analysis, in which only limited descriptive evidence is presented.

Following substantive commencement, future research should be carried out on complaints and decisions, with appropriate permissions and privacy protections. A claimant study might examine the character of alleged injury, evidence availability, length of proceeding and abandoning of claims. Regional and language diversity should be sampled as well as different types of non-filing. This correlation with anonymous institutional results could be used to determine if formal remedies can be made practical. An assessment of deterrence would also need to involve some defensible comparison technique and consideration of issues of changes in reporting and detection.

12.CONCLUSION

In the Indian understanding of the constitution, there are interests which, whenever detriment is caused, need not be expressed as monetary loss but which, when the detriment is committed, shrivels and needs to be protected. While interests may be protected under the enforcement framework of the DPDP Act, there is no specific compensation entitlement from



the application of large regulatory penalties. While current remedies are still applicable under specific situations, a disjointed path to remedy continues during the commencement transition.

Official statistics are a credible representation of the cybersecurity that has been documented, but there remains controversy regarding privacy injury and its incidence. There, Indian scholarship and comparative jurisprudence have shown the need for a defensible theory of non-material harm, credible evidence of causation, access to the evidence of organizations and a forum open to awarding adequate relief. The proposed framework is based on express law and proportional procedure to ensure these requirements are directly linked. The added value it brings in the context of the broader doctoral thesis lies in the concrete approach towards measuring the relevance of data protection law for the stake of the privacy rights with restoring accessibility. Assessment of effective protection should be based on the person affecter's capacity to create an injury and get a rational response tailored to the injury.

REFERENCES

1. Digital Personal Data Protection Act, 2023, Act 22 of 2023, especially sections 8, 13, 17, 27, 31, 32, 34, 38, 39 and 44(2), and the Schedule.
2. Justice K. S. Putt swamy (Retd.) v Union of India (2017) 10 SCC 1, especially the discussion of dignity, autonomy and informational privacy in the opinion of Chandrachud J and the Court's final order.
3. Ministry of Home Affairs, "Assistance to States to Tackle Cyber Incidents", written reply to the Lok Sabha, Press Information Bureau, 24 March 2026, Release ID 2244504. Official CERT-In annual counts for 2021-2025.
4. Bhairav Acharya, "The Four Parts of Privacy in India" (2015) 50(22) Economic and Political Weekly 32-38.
5. Helen Nissenbaum, "Privacy as Contextual Integrity" (2004) 79 Washington Law Review 119.
6. Danielle Keats Citron and Daniel J Solove, "Privacy Harms" (2022) 102 Boston University Law Review 793, especially 819-862.
7. Ajay Kumar Bisht and Neeruganti Shanmuka Sreenivasulu, "Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023", in Jaydip Sen (ed.), Data Privacy: Techniques, Applications, and Standards (IntechOpen, 2024), especially section 5.2. DOI: 10.5772/intechopen.1007353.
8. Kriti Kabra, "What About Me? Making a Case for Individual Compensation under India's Digital Privacy Framework" (Tech Law Forum at NALSAR, 6 August 2026). Scholarly commentary.
9. Sana Athar, Devashish Gosain, Anja Feldmann, Mannat Kaur and Ha Dao, "Nobody Should Control the End User: Exploring Privacy Perspectives of Indian Internet Users in Light of DPDPA" (2025), arXiv:2508.17962, version 1, especially sections 3, 4 and 5.3. Author manuscript consulted.
10. Ministry of Electronics and Information Technology, Notification G.S.R. 843(E), Gazette of India, 13 November 2025, clauses (a)-(c).
11. Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, 13 November 2025, rules 1, 6, 7 and 14.
12. Information Technology Act, 2000, Act 21 of 2000, sections 43A and 46, India Code consolidated text as on 27 June 2025; read with commencement notification in reference 10.
13. Nilabati Behera v State of Orissa (1993) 2 SCC 746.
14. R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632, especially paragraph 26.
15. Consumer Protection Act, 2019, Act 35 of 2019, sections 2(7), 2(42) and 2(47)(ix). Statutory text reproduced at:
16. L Chandra Kumar v Union of India (1997) 3 SCC 261.
17. Regulation (EU) 2016/679, General Data Protection Regulation, [2016] OJ L119/1, articles 77-82 and recital 146.
18. UI v Österreichische Post AG, Case C-300/21, EU:C:2023:370, 4 May 2023, paragraphs 32, 42 and 51.
19. VB v Natsionalna agentsia za prihodite, Case C-340/21, EU:C:2023:986, 14 December 2023, paragraphs 75-86.
20. IP v Quirin Privatbank AG, Case C-655/23, EU:C:2025:655, 4 September 2025, paragraphs 53-64.
21. Brillen Rottler GmbH & Co. KG v TC, Case C-526/24, EU:C:2026:216, 19 March 2026, paragraphs 58-67.
22. Lloyd v Google LLC [2021] UKSC 50, especially paragraphs 8 and 115.
23. Reed, Michael v Bellingham, Alex (Attorney-General, intervener) [2022] SGCA 60, especially paragraphs 107-116.
24. Personal Data Protection Bill, 2019, Bill 373 of 2019, clauses 3(20) and 64, as introduced in Lok Sabha. This is a legislative proposal, not the operative Act.