# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

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



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


## CYBER LAWS IN INDIA


***~ Pal Meena***


There is no universally accepted definition of cybercrime, since it is an innovation of modern technology and is still evolving. However, the definition that could be drawn from various cyber frameworks includes elements common to existing cybercrime definitions. Cybercrime is an act that violates the law, which is perpetrated using information and communication technology (ICT) to target networks, systems, data, websites and/or technology or facilitate a crime. Cybercrime differs from traditional crime in that it "knows no physical or geographic boundaries" and can be conducted with less effort, greater ease, and at greater speed than traditional crime.[1]

Cyber law in India is primarily governed by the Information Technology Act, 2000, also known as the mother legislation in the field of electronic crime. It defines specific offences and assigns penalties addressing various electronic crimes such as hacking, data theft, tampering, cyber terrorism, etc. Other legislation that holds relevance in this field is the Constitution of India and the Bharatiya Nyaya Sanhita, 2023, which supplements traditional criminal jurisprudence with modern provisions. The IT Rules & Directives provide intermediary guidelines and mandatory incident reporting frameworks overseen by agencies like CERT-In.

With the increasing frequency and sophistication of cybersecurity breaches, the question of protection of personal data has raised wider legal accountability and individual rights. Nowadays, banks, financial institutions, healthcare providers, investment platforms, telecommunications companies and other digital intermediaries routinely collect and store highly sensitive personal and financial information of users. When these institutions suffer a

[1] UNODC, https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-1/key-issues/cybercrime-in-brief.html (last visited Oct. 5, 2026)

cyberattack, the consequences extend beyond the organisation and affect the users, directly or indirectly. Consequently, it is the individuals who face the threats to their personal data, which would likely result in the ultimate risk of various cyber threats such as identity theft, phishing, financial fraud, impersonation, reputational harm and the list goes on. Unfortunately, India's legal framework has not been able to evolve considerably in response to these risks. Keeping up with these cyber attackers is becoming more and more of a challenge, as, with the rapid development of artificial intelligence, their methods are becoming innovative and unpredictable. However, the various legal frameworks, such as the IT Act, the CERT-In Cyber Security Directions, 2022, the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025, impose obligations concerning cybersecurity and personal data protection on these institutions, a significant question remains: what immediate effective legal remedy is available to an individual whose personal data has been compromised in a cybersecurity breach, particularly where the breach has not yet resulted in demonstrable financial loss?

This paper examines the position of individuals affected by cybersecurity breaches under the Indian legal system and evaluates the relationship between cybersecurity obligations, data-protection duties and individual remedies. It analyses the statutory framework governing reasonable security safeguards, breach notification, regulatory reporting, grievance redressal and financial liability. It also examines the emerging judicial response to large-scale cyberattacks, including the Bombay High Court's 2026 decision concerning a ransomware attack on HDFC Asset Management Company. The paper argues that India's framework has become considerably stronger in imposing obligations upon organisations but remains comparatively underdeveloped in providing direct, accessible and proportionate remedies to individuals for the privacy and security harms caused by a breach. The paper proposes a victim-centric remedial framework based on mandatory and meaningful breach notification, effective grievance mechanisms, risk mitigation duties, clearer compensation principles, sector-specific protection and recognition of non-financial harm.

**Keywords:** Cybersecurity, Data Breach, Personal Data, Digital Personal Data Protection Act, CERT-In, Privacy, Cyber Law, Data Principal, Legal Remedies, Ransomware.

## INTRODUCTION

The current digital economy operates on a basic exchange: individuals provide personal information in return for access to banking, insurance, healthcare, telecommunications,

education, employment, commerce and other services. The scale of this exchange and the way all these documents have become so interconnected that it has fundamentally altered the nature of privacy. Now your mobile number and email are attached not only to your bank account, AADHAAR, PAN, etc., but also to various social media applications. So the problem is that personal information is no longer merely contained in individual records but is continuously collected, aggregated, analysed, stored and transferred across interconnected digital systems.

This creates a greater legal problem; an individual may take reasonable precautions to protect their own information and yet remain vulnerable because the information is also held by another organisation. A bank stores a customer's account details, PAN, address, mobile number and transaction information. An investment company may hold identity documents, bank details, portfolio information and contact information. A healthcare provider may possess information considerably more sensitive than ordinary financial records. The problem arises when this information is stored on compromised digital cloud storage. The security of such information is therefore dependent not only upon the individual's behaviour but upon the cybersecurity practices of the institution entrusted with it.

Sometimes, the consequences of a cybersecurity breach can be significantly broader than the immediate loss suffered by the organisation that was attacked; a ransomware attack against a financial institution, for example, may involve the exfiltration of customer information, as seen in the case of HDFC AMC v. Union of India & Ors.[2] Even where the institution restores its systems, and no money has immediately disappeared from customers' accounts, the individuals whose data has been stolen remain exposed to various forms of secondary victimisation.

In May 2026, the Bombay High Court considered an urgent application following an alleged ransomware attack on HDFC Asset Management Company in which more than 680 GB of data was claimed to have been exfiltrated. The material allegedly included names, addresses, identity documents, PAN details, bank account details, portfolio and investment information, mobile numbers and email addresses belonging to millions of investors and other stakeholders. The company had reported the incident to SEBI and CERT-In and sought urgent judicial intervention to prevent further dissemination of the stolen information. The Court recognised the serious risk of identity theft, financial fraud, phishing, SIM-swapping and

[2] *HDFC Asset Management Company Limite*d v. *Union of India and Others (2026) Bom.*

unauthorised transactions and granted interim relief against the use and dissemination of the stolen data. The case demonstrates an important distinction. A cyberattack may be directed against an institution, but its consequences are borne by individuals.

Although India's regulatory framework has increasingly concentrated on preventing this harm, for example, Section 70B of the Information Technology Act, 2000,[3] empowers the Indian Computer Emergency Response Team (CERT-In) to coordinate cybersecurity responses. The CERT-In Directions of 2022 require specified cyber incidents, including data breaches and data leaks, to be reported within six hours. The Digital Personal Data Protection Act, 2023 further establishes obligations upon Data Fiduciaries to adopt reasonable security safeguards and provides an institutional mechanism through the Data Protection Board.

The Digital Personal Data Protection Rules, 2025, represent another significant development, requiring a Data Fiduciary, upon becoming aware of a personal data breach, to notify affected Data Principals without delay in clear and plain language, including information concerning the nature and extent of the breach, likely consequences, mitigation measures and safety measures that the affected person can take. The Data Fiduciary must also notify the Board and provide detailed information within the prescribed period.

Yet a critical question remains unanswered in practical terms: What happens to the individual after the notification?

Knowing that one's data has been compromised does not itself restore privacy; it does not prevent the information from being circulated elsewhere; nor does it necessarily compensate an individual for the mental stress, loss of control, increased exposure to fraud or the costs of protecting oneself from future misuse.

This paper therefore examines whether India's emerging data-protection and cybersecurity framework provides an effective remedy to individuals affected by cybersecurity breaches.

## THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000, remains the principal statutory foundation of the cyber-law framework in India. Although it was enacted with the objective of providing legal recognition to electronic transactions and facilitating electronic governance, over the years, it

[3] Information Technology Act, No. 21 of 2000, § 70B (Ind.).

has been broadened through amendments to become important legislation for dealing with various forms of cybercrime and unlawful use of computer resources.

Section 43 of the Act[4] provides civil liability for specified acts involving computer resources, including unauthorised access and extraction or copying of data. Section 43A[5] addresses compensation for failure by a body corporate to implement reasonable security practices and procedures in relation to sensitive personal data or information. Section 66[6] of the Act also provides for criminal offences relating to unauthorised access and other forms of computer-related misconduct.

The importance of the IT Act for cybersecurity breaches lies partly in its recognition that inadequate protection of information can have legal consequences. However, the provisions concerning organisational responsibility do not provide a complete framework for dealing with the continuing consequences of large-scale personal-data breaches, as it was not designed as comprehensive personal-data protection legislation.

## CERT-IN AND MANDATORY INCIDENT REPORTING

Section 70B of the IT Act establishes CERT-In as the national agency responsible for specified cybersecurity functions. Its role includes the collection, analysis and dissemination of information concerning cyber incidents, forecasting and issuing alerts, coordinating emergency measures and responding to cyber incidents.

The 2022 CERT-In Directions significantly strengthened this framework. They require covered entities to report specified cyber incidents within six hours of noticing them. CERT-In expressly identifies data breaches and data leaks among incidents requiring reporting within the stipulated period. The framework therefore operates primarily from a systemic cybersecurity perspective. Its objective is to ensure that the State has timely information about cyber incidents so that it can identify threats, coordinate responses and improve national cyber resilience, which is essential, but reporting an incident to CERT-In is fundamentally different from providing a remedy to the individual affected by that incident.

CERT-In primarily addresses the first problem; it helps the state understand and respond to the cyber incident. It does not establish a comprehensive mechanism through which an affected individual can claim relief for the loss of control over their personal information.

[4] Information Technology Act, No. 21 of 2000, § 43 (Ind.).
[5] Information Technology Act, No. 21 of 2000, § 43A (Ind.).
[6] Information Technology Act, No. 21 of 2000, § 66 (Ind.).

Thus, although the CERT-In framework strengthens institutional accountability, it does not answer the question that is at the centre of this paper: what happens to the individual after their data has been compromised?

## THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The DPDP Act represents India's most significant attempt to establish a comprehensive framework for digital personal data protection. The Act places obligations upon data fiduciaries. Among the core obligations is the requirement to take reasonable security safeguards to prevent personal-data breaches.

The Act also provides for breach notification and establishes the Data Protection Board. Section 27[7] empowers the Board to enquire into personal-data breaches, including on a complaint made by a Data Principal, and to impose penalties and issue directions. This is an important development because it gives the affected individual a regulatory route rather than requiring every victim to independently pursue conventional civil litigation.

A penalty imposed upon a Data Fiduciary serves a public regulatory function. It may deter future non-compliance and hold the organisation accountable. But a penalty does not necessarily compensate the individual whose information has been exposed. This raises a central question: does the DPDP framework sufficiently connect institutional accountability with individual redress?

## THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

The DPDP Rules, 2025, strengthen the breach-notification framework considerably. When a data fiduciary becomes aware of a personal data breach, the affected data principal must be informed without delay. The notification must describe the nature, extent and timing of the breach, likely consequences, mitigation measures and safety measures that the individual may adopt. A contact person must also be identified for queries.

The Data Fiduciary must separately inform the Data Protection Board. The framework also requires detailed information concerning the circumstances leading to the breach, mitigation, remedial measures and the notification provided to affected individuals. This is an important improvement over a system in which individuals might never know that their information had been compromised. However, notification cannot be treated as synonymous with remedy.

[7] The Digital Personal Data Protection Act, 2023, § 27(Ind.).

Consider a hypothetical example. A bank suffers a sophisticated cyberattack. The attacker obtains the customer's name, PAN, address, mobile number, bank account details and identity documents. The bank discovers the breach and promptly notifies the customer. The customer has suffered no unauthorised debit. What is the remedy? The individual may be advised to change passwords, monitor accounts, beware of phishing and report suspicious activity. But the person's information cannot simply be “recalled” from the attacker. Once identity documents and financial information have entered an uncontrolled digital environment, the risk may persist indefinitely. Thus, notification is a necessary remedy but not a complete remedy.

## THE CENTRAL GAP: LIABILITY WITHOUT AN IMMEDIATE FINANCIAL LOSS

The most significant gap examined by this paper concerns the situation in which personal data is compromised, but the individual cannot demonstrate immediate financial loss. Existing financial-protection mechanisms are comparatively clearer where an unauthorised electronic transaction has occurred. For example, RBI's customer-protection framework provides mechanisms for reporting unauthorised electronic transactions and establishes circumstances in which customers may have zero or limited liability. In cases of certain third-party breaches, timely reporting can result in zero liability, and banks are required to provide mechanisms for reporting and acknowledging unauthorised transactions. The burden of proving customer liability also lies on the bank. This framework is important but operates primarily around unauthorised transactions. The problem examined here arises earlier. What if the data has been stolen, but no money has yet been stolen? The victim may nonetheless face substantial and continuing risk. This demonstrates a gap between financial harm and informational harm.

A person's PAN, identity document, address, mobile number or financial profile can be exploited without producing an immediate bank-account debit. Identity theft may occur months later. Phishing may become more sophisticated because the attacker possesses genuine personal information. Fraudulent loans or accounts may potentially be created using stolen credentials. The legal system therefore faces a temporal problem: the harm may be real before it becomes financially measurable. A purely loss-based remedial framework risks requiring the victim to wait until the predicted harm actually occurs.

## THE RIGHT TO PRIVACY AND DATA BREACHES

In 2017, a constitutional bench of nine judges of the Supreme Court of India in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[8] upheld that privacy is a fundamental right, which is entrenched in Article 21[9] (Right to Life & Liberty) of the Constitution of India. Personal information forms an important component of informational privacy. The State's recognition of privacy as a constitutional value provides an important foundation for understanding why unauthorised disclosure of personal data is not merely a commercial inconvenience. Most cybersecurity breaches involving banks, insurers and private companies are attacks perpetrated by third parties. The institution holding the information may itself be a victim of the crime. The difficult legal question is therefore: When should an institution be responsible for a breach caused by a third-party cybercriminal?

A simplistic approach would make every hacked organisation automatically liable, which would be problematic. Cybersecurity threats can be sophisticated, constantly evolving and sometimes impossible to eliminate completely. The opposite approach, however, would also be unsatisfactory: "The hacker did it; therefore, the organisation bears no responsibility." Such an approach could undermine the very concept of institutional accountability.

Therefore, the appropriate legal test is whether the organisation implemented reasonable and proportionate security measures appropriate to the nature and sensitivity of the data it controlled. The DPDP framework's emphasis on reasonable security safeguards provides the basis for such an approach.

## THE HDFC ASSET MANAGEMENT RANSOMWARE CASE

The 2026 Bombay High Court proceedings involving HDFC Asset Management Company provide a contemporary illustration. The company approached the court after an alleged ransomware group claimed to have exfiltrated more than 680 GB of data. The information allegedly included sensitive personal and financial information relating to investors. The company reported the incident to SEBI and CERT-In and sought urgent relief preventing further use and dissemination of the stolen material. The Court found a prima facie case and recognised that dissemination of the information could produce serious and irreversible consequences, including identity theft, financial fraud, phishing, SIM-swapping and unauthorised financial transactions. It granted interim relief restraining the use, publication, distribution and disclosure of the stolen information and directed relevant authorities to take

[8] *Justice K.S. Puttaswamy (Retd.)* v. *Union of India* (2017) 10 SCC 1.
[9] India Const. art. 21.

steps to remove or disable identified accounts and other digital locations associated with the stolen material.

The case is significant for two reasons. First, it demonstrates that Indian courts can provide rapid injunctive relief in response to cyberattacks. Second, it illustrates the limits of such relief.

The Court's order primarily protects the confidentiality of the stolen data and attempts to prevent further dissemination. It could not restore the information to the individual or eliminate the risk that copies may already exist elsewhere. This reveals the distinctive nature of cybersecurity harm. A stolen physical object can potentially be recovered. A stolen database can be copied indefinitely. Consequently, conventional notions of restitution may be insufficient.

**WHO SHOULD BEAR THE COST OF POST-BREACH PROTECTION?**

A further unresolved question is the allocation of post-breach costs. Suppose an institution's cybersecurity failure exposes thousands of customers to identity theft.

Should customers themselves have to:

- monitor their credit reports;
- change credentials;
- replace identity documents;
- contact banks;
- obtain legal assistance;
- monitor suspicious transactions;
- protect themselves from phishing attempts; and
- bear the psychological burden of knowing that their information is circulating?

Or should the institution be held responsible for safeguarding the information bear at least some of these costs?

A victim-centric model should recognise that cybersecurity is not merely an organisational IT expense. When organisations collect extensive personal information as part of their business

models, security becomes part of the legal responsibility associated with holding that information.

This does not justify automatic liability. Instead, liability depends upon:

1. the sensitivity of the data;
2. the scale of the breach;
3. the foreseeability of the risk;
4. the security measures adopted;
5. whether known vulnerabilities were ignored;
6. the speed and adequacy of the response;
7. the quality of notification; and
8. the actual or reasonably foreseeable harm to Data Principals.

**THE PROBLEM OF MULTIPLE OVERLAPPING FRAMEWORKS**

Another difficulty is fragmentation. An individual affected by a cybersecurity breach may potentially encounter:

- the IT Act;
- the DPDP Act;
- CERT-In requirements;
- RBI regulations;
- SEBI cybersecurity requirements;
- contractual remedies;
- consumer-protection mechanisms;
- constitutional privacy principles; and
- ordinary civil and criminal law.

The existence of multiple laws is not inherently problematic. Cybersecurity itself is cross-sectoral. The problem arises where an individual cannot easily determine: Which authority should I approach? An organisation may simultaneously be required to report an incident to CERT-In, a sectoral regulator and the Data Protection Board, while the individual victim may have a separate grievance mechanism.

The legal architecture therefore risks becoming institution-centric rather than victim-centric. A mature data-protection framework should not require an ordinary individual to understand the institutional division between CERT-In, the Data Protection Board, RBI, SEBI and other regulators before obtaining meaningful assistance.

## PROPOSED REFORMS

### A. A clear statutory right to breach-related assistance

The law should recognise that breach notification alone is insufficient in cases involving significant risk. Where sensitive personal or financial information is compromised, the Data Fiduciary should be required to provide reasonable assistance to affected individuals.

Depending on the circumstances, this could include:

- dedicated helplines;
- assistance in securing compromised accounts;
- identity-theft support;
- credit-monitoring assistance in high-risk cases;
- replacement or reissuance support for compromised credentials where appropriate; and
- continuing updates regarding material developments.

### B. A risk-based compensation framework

Compensation should not depend exclusively upon proof of direct monetary loss. A more nuanced framework could distinguish between:

**Level I — Exposure without material foreseeable risk**

Minimal remedy, primarily notification and information.

**Level II — Exposure involving sensitive identity or financial information**

Enhanced mitigation and assistance.

**Level III — Exposure creating substantial risk of identity theft or financial fraud**

Enhanced institutional responsibility and potentially compensation.

**Level IV — Demonstrated financial or other serious harm**

Full remedial and compensatory mechanisms, subject to proof and applicable law.

Such a framework would recognise that the seriousness of a breach can be assessed before the worst consequence materialises.

**C. A clearer relationship between regulatory penalties and individual compensation**

Regulatory penalties serve deterrence. Compensation serves restoration. These objectives should not be conflated. If the Data Protection Board imposes a penalty upon a Data Fiduciary, the legal framework should clearly address whether and how affected individuals can obtain compensation or other forms of individual relief. Otherwise, a person whose data was compromised may witness a large penalty being imposed upon an organisation while receiving no meaningful remedy personally.

**D. Sector-specific protection for high-risk data**

Not all data breaches are equally harmful. The compromise of a public email address is fundamentally different from the compromise of:

- bank-account information;
- PAN;
- identity documents;
- health information;
- biometric information;
- financial portfolios; or
- combinations of information capable of facilitating identity theft.

The legal response should therefore become more stringent as the sensitivity and exploitability of the information increases. The HDFC Asset Management case illustrates this principle particularly clearly because the allegedly compromised information included identity documents and financial information relating to investors.

**E. Mandatory meaningful notification**

Notification should not become a formal compliance exercise. A statement such as "your data may have been compromised; please remain vigilant" does little to empower the victim. The affected individual should be told, to the extent known:

- what information was compromised;
- when the breach occurred;
- when it was discovered;
- how the breach occurred;
- what risks are reasonably foreseeable;
- what the organisation has done;
- what the individual should do; and
- whom the individual can contact.

The 2025 Rules already move significantly in this direction by requiring information concerning the nature and extent of the breach, consequences, mitigation and recommended safety measures. The next step should be ensuring meaningful implementation.

## CONCLUSION

India's cybersecurity framework has undergone significant transformation. The CERT-In Directions have strengthened institutional incident reporting; the Digital Personal Data Protection Act has established a dedicated statutory framework for personal-data protection; and the Digital Personal Data Protection Rules, 2025 have added greater specificity concerning breach notification and security safeguards. The legal problem, however, has not disappeared.

A cybersecurity breach creates a peculiar form of harm because information, unlike a physical object, can be copied indefinitely. The institution may recover its systems, the attacker may disappear, and the organisation may report the incident to regulators, while the individual whose data was compromised continues to face an uncertain risk.

The emerging legal framework therefore needs to move beyond the question of whether an organisation complied with its reporting obligations. It must also ask: what does the law owe to the person whose data has been exposed?

The distinction between institutional accountability and individual remedy is central. CERT-In reporting serves national cybersecurity. Regulatory penalties serve deterrence and compliance. Judicial injunctions can restrict dissemination. Banking regulations can protect customers from certain unauthorised transactions. Yet none of these mechanisms, individually, constitutes a complete remedy for the individual whose personal information has entered the hands of cybercriminals.

The problem becomes particularly acute where no immediate financial loss has occurred. A victim may have lost control over highly sensitive personal information without being able to point to a specific monetary injury. Waiting until identity theft or financial fraud actually occurs before recognising legal harm would place the burden of cybersecurity failure disproportionately upon individuals.

The DPDP framework provides an important foundation for addressing this problem. Its recognition of reasonable security safeguards, breach notification and individual grievance mechanisms marks a substantial advance in Indian data protection. The 2025 Rules further strengthen the position of data principals by requiring timely and meaningful information following a breach. However, India's next stage of development should focus on effective remedies rather than merely regulatory obligations.

A comprehensive victim-centric model should combine mandatory meaningful notification, risk-based assistance, proportionate compensation, sector-specific safeguards and accessible grievance mechanisms. It should also clarify the relationship between regulatory penalties and individual compensation. Ultimately, the objective of cybersecurity law should not be limited to protecting databases. It must protect the people whose lives are represented inside those databases.

The measure of an effective cybersecurity framework should therefore not be merely how quickly a breach is reported, how much a regulator can penalise an organisation, or how effectively a court can order stolen information to be removed. Its ultimate measure should be whether the individual whose data has been compromised is given a meaningful opportunity to understand the harm, reduce the resulting risk and obtain an effective remedy.

India has taken important steps towards that objective. The remaining challenge is to ensure that, when the next major breach occurs, the individual is not left with nothing more than a notification saying that their data may have been stolen.

**Authorities and references**

1. UNODC, https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-1/key-issues/cybercrime-in-brief.html (last visited Oct. 5, 2026)
2. HDFC Asset Management Company Limited vs Union of India and Others (2026) Bom.
3. Information Technology Act, No. 21 of 2000, §§ 70B, 43, 43A, 66 (Ind.).
4. The Digital Personal Data Protection Act, 2023, § 27(Ind.).
5. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.
6. India Const. art. 21.