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

LEGAL ASPECTS OF CYBER SECURITY IN INDIA: EMERGING CHALLENGES AND THE REGULATORY FRAMEWORK

DIVYANSHA SINGH

I. INTRODUCTION

Much of everyday life in India now depends on digital systems. Bank transfers, land records, medical prescriptions, school admissions, tax filings, even grocery shopping all of it now runs at least in part through a digital system somewhere. This shift has happened quickly and it has outpaced the public's general understanding of how exposed these systems actually are. A country that digitizes faster than it secures itself is almost by definition creating new categories of risk alongside every new convenience.

That risk has materialized in familiar ways for example financial fraud carried out through fake payment links, personal data siphoned off through poorly secured servers, identities stolen and misused, critical systems like banks, hospitals, even government departments disrupted by attacks that did not require a single person to be physically present at the scene.[1] They are no longer isolated incidents but recurring features of India's digital landscape.

What makes this a legal problem and not merely a technical one that each of these incidents raises questions that the law is meant to answer. Who is liable when a breach occurs the attackers, the platforms or the institutions that failed to secure their systems? What counts as consent when data is collected through an app most users never read the terms of? Where does a prosecution even begin when the servers, the attacker and the victim are located in three different countries? India's

[1] Sukrati Sharma & Yashasvi Panwar, *Behind the Screen: The Human Cost of Cybercrime in India*, 7(4) Indian J.L. & Legal Rsch. 5832 (2025).

answer to these questions has developed unevenly built primarily around the Information Technology Act, 2000, a statute drafted at the time when none of this was yet urgent and supplemented since then by amendments, regulatory directions and most recently a dedicated data protection law.

This article examines whether that accumulated framework is equal to the task. It considers the statutory provisions currently in force, the constitutional boundaries courts have placed on their use, the practical difficulties that arise in enforcing them and the reforms necessary to bridge the gap between the existing legal framework and its effective enforcement.

II. THE LEGAL FRAMEWORK GOVERNING CYBER SECURITY IN INDIA

A. THE INFORMATION TECHNOLOGY ACT, 2000

India's principal cyber law statute is the Information Technology Act, 2000 enacted to give legal recognition to electronic transactions and digital signatures.[2] Its scope has since expanded well beyond that original commercial purpose. Section 43[3] fixes civil liability on anyone who gains unauthorized access to a computer, computer system or network requiring the wrongdoer to compensate the affected person. Section 66[4] criminalizes the same acts where committed dishonestly or fraudulently carrying up to three years of imprisonment and a fine of up to five lakh rupees or both. Together, these provisions establish the Act's basic proposition that unauthorized interference with a computer system is unlawful, whether the remedy sought is compensation or punishment.

B. CYBER OFFENCES UNDER THE INFORMATION TECHNOLOGY ACT, 2000

The Act also creates offence specific provisions for particular forms of harm. Section 66E penalizes capturing or transmitting images of a person's private areas without consent[5].

---

[2] Sukrati Sharma & Yashasvi Panwar, *Behind the Screen: The Human Cost of Cybercrime in India*, 7(4) Indian J.L. & Legal Rsch. 5832 (2025).
[3] The Information Technology Act, 2000, No. 21 of 2000, § 43 (India).
[4] The Information Technology Act, 2000, No. 21 of 2000, § 66 (India).
[5] The Information Technology Act, 2000, No. 21 of 2000, § 66E (India).

Section 66F[6] addresses cyber terrorism, prescribing life imprisonment for acts using computer resources that threaten India's sovereignty or security or spread terror among the public. Section 67[7] and 67A[8] deal with the obscene and sexually explicit material with escalating penalties for repeat offences. Section 72[9] protects the confidentiality of information accessed under the Act's regulatory powers. Together these provisions calibrate liability according to the gravity of the harm from individual privacy violations to threats against national security.

C. SHREYA SINGHAL V. UNION OF INDIA AND THE CONSTITUTIONAL LIMITS OF CYBER REGULATION

Not every attempt to regulate online conduct has survived judicial scrutiny. Section 66A[10] criminalized sending information that was "grossly offensive" or caused "annoyance" or "inconvenience". In *Shreya Singhal v. Union of India*[11] the Supreme Court of India struck down the provision entirely holding its language too broad and vague in violation of Article 19(1)(a) of the constitution. The judgment established that cyber regulation cannot rely on open ended language merely because the medium is digital, the same constitutional standards of clarity and proportionality that govern offline speech apply online as well.

D. CERT-IN AND THE CERT-IN DIRECTIONS, 2022

Section 70B[12] establishes CERT-In as the national agency for collecting and disseminating information on cyber incidents and coordinating India's response to them. In April 2022, CERT-In directed service providers, intermediaries and government organisations to report specified cyber incidents within six hours and to retain system logs for a prescribed period.[13] This marked a shift from a largely voluntary reporting culture to a mandatory,

---

[6] The Information Technology Act, 2000, No. 21 of 2000, § 66F (India).
[7] The Information Technology Act, 2000, No. 21 of 2000, § 67(India).
[8] The Information Technology Act, 2000, No. 21 of 2000, § 67A (India).
[9] The Information Technology Act, 2000, No. 21 of 2000, § 72 (India).
[10] The Information Technology Act, 2000, No. 21 of 2000, § 66A (India).
[11] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[12] The Information Technology Act, 2000, No. 21 of 2000, § 70B (India).
[13] Indian Computer Emergency Response Team, Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet (Apr. 28, 2022).

time bound one, reflecting the reality that delayed reporting undermines both individual remedies and any wider institutional response.

Although these provisions establish the foundation of India's cyber security framework, their effectiveness is increasingly tested by the pace of evolving threats. The following section examines the principal challenges this framework now faces.

III. EMERGING CHALLENGES IN INDIA'S CYBER LANDSCAPE

A. FINANCIAL CYBER FRAUD

Financial fraud has emerged as one of the fastest growing categories of cybercrime under the Information Technology Act driven largely by the rapid expansion of India's digital payments ecosystem, including the Unified Payments Interface and the other instant payment systems.[14] Phishing remains the most common entry point a message or call convincing enough that a user discloses a onetime password, card number or login credentials later used to authorize transactions that appear from the bank's system indistinguishable from ones the account holder made themselves. This creates a practical difficulty under Section 66 since the "unauthorized access" it contemplates is often preceded by consent obtained through deception rather than technical intrusion conduct the provision was not originally drafted to capture.

B. CYBERSTALKING AND IDENTITY BASED OFFENCES

A related category of harm involves the misuse of identity and the persistent monitoring of a person's online activity. Indian courts recognized cyberstalking even before any legislation expressly addressed it. In the Ritu Kohli matter, a man impersonated a woman online circulated her phone number and invited strangers to contact her leading to a stream of obscene calls an episode that predates India's cyberstalking jurisprudence by more than a decade.[15] A comparable pattern arose in State of *Tamil Nadu v. Suhas Katti*[16] where a fabricated email account was used to invite harassment of the victim and the accused was prosecuted under

[14] Sukrati Sharma & Yashasvi Panwar, *Behind the Screen: The Human Cost of Cybercrime in India*, 7(4) Indian J.L. & Legal Rsch. 5832 (2025).
[15] *Id.*
[16] Nikita Sharma & Sakshi Vadhera, *Case Commentary: State of Tamil Nadu vs. Suhas Katti* (Jan. 31, 2021) (unpublished manuscript), available at SSRN: https://ssrn.com/abstract=3776961.

Section 67 of the IT Act read with the Indian Penal Code. Both cases predate any provision drafted specifically for stalking showing how courts have had to stretch obscenity and privacy provisions to reach conduct that is in substance about intimidation and misuse of digital identity.

C. INTERMEDIARY LIABILITY AND ONLINE PLATFORMS

A further challenge concerns the platforms through which such conduct is carried out. Section 79[17] grants intermediaries conditional immunity from liability for user generated content provided they neither initiated the transmission nor selected or modified it and complied with prescribed due diligence requirements. This safe harbour is essential to how the internet functions but it has generated disputes over where due diligence ends and complicity begins. In *Shreya Singhal* the Supreme Court held that an intermediary's obligation to act arises only upon actual knowledge of a judicial or government removal order, not a private complaint.[18] This protects against arbitrary censorship, but also means harmful content may remain online until such a direction is secured a delay capable of significantly aggravating harm in cases involving ongoing harassment or nonconsensual imagery.

IV. ENFORCEMENT CHALLENGES AND INSTITUTIONAL GAPS

A. CROSS-BORDER ENFORCEMENT

A significant share of cybercrime affecting Indian victims originates at least in part outside India's territorial jurisdiction servers hosted abroad, payment gateways routed through foreign intermediaries or perpetrators operating from jurisdictions with limited cooperation. The IT Act extends its application to offences committed outside India where the conduct involves a computer system located within the country, but jurisdiction on paper does not resolve the practical difficulty of securing evidence, identifying an accused or compelling foreign providers to cooperate.[19] Mutual legal assistance treaties exist for this purpose but are frequently slow while cybercrime evidence such as server logs, IP addresses, transaction trails can be altered or deleted long before a formal request is processed. The result is a structural

[17] The Information Technology Act, 2000, No. 21 of 2000, § 79 (India).
[18] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[19] The Information Technology Act, 2000, No. 21 of 2000, § 75 (India).

mismatch between the speed of the offence and the pace at which cross border legal mechanisms can respond.

B. INSTITUTIONAL LIMITATIONS

Even where jurisdiction is clear, India's capacity to investigate cybercrime at the pace it occurs remains uneven. Digital forensics requires specialised training and equipment that many state and district police units still lack and reported cases have grown far faster than investigative capacity.[20] A complaint may be registered promptly but tracing an attacker or preserving usable digital evidence often lags well behind. The National Cyber Crime Reporting Portal has streamlined complaint filing but registering a complaint and resolving it remain two different things a gap that persists as one of the framework's most significant institutional weaknesses.

C. LESSONS FOR INDIA'S CYBER SECURITY FRAMEWORK: THE COSMOS BANK CYBERATTACK

The 2018 Cosmos Bank attack illustrates how these gaps converge. Over roughly seven hours, attackers who had compromised the bank's ATM switching and SWIFT messaging systems carried out more than 12,000 fraudulent ATM withdrawals and over 2,800 fraudulent transactions, cloning cards and bypassing real-time verification.[21] The incident did not stem from a single catastrophic failure but from the combination of ordinary vulnerabilities inadequate segregation between banking and payment systems, weak real time monitoring that together enabled a coordinated, automated attack faster than conventional responses could contain.

These gaps point towards institutional and coordination reforms rather than further legislative change. The following sections considers what such reform might look like.

V. TOWARDS A STRONGER REGULATORY FRAMEWORK

[20] Sukrati Sharma & Yashasvi Panwar, *Behind the Screen: The Human Cost of Cybercrime in India*, 7(4) Indian J.L. & Legal Rsch. 5832 (2025).
[21] Id

Closing the gaps identified above requires several coordinated reforms most of which strengthen how the existing framework operates rather than what it prohibits.

A. INTEGRATING THE IT ACT WITH THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The IT Act and the DPDP Act currently operate along parallel tracks, the former addressing unauthorized access and computer related offences the latter governing the collection and protection of personal data, yet a single breach often implicates both regimes at once.[22] A company that suffers a cyberattack may face an IT Act investigation into the intrusion and a DPDP Act inquiry into its safeguards simultaneously. Clearer coordination between the two regimes, including shared timelines and consistent breach notification standards would reduce duplication and give affected parties a more coherent process.

B. STRENGTHENING CERT-IN'S OPERATIONAL ROLE

The six hour reporting requirement under the CERT-In directions, 2022 was a meaningful step but its value depends on how quickly reported information is analysed and acted upon.[23] A reporting obligation without operational capacity risks becoming a formality rather than an early warning system. Strengthening CERT-In's ability to issue real time advisories and coordinate directly with sectoral regulators such as the RBI and SEBI would convert reporting into genuine response capacity.

C. BUILDING INSTITUTIONAL CAPACITY AT THE STATE LEVEL

Most cybercrime investigations are conducted by the state and district police units not central agencies. Digital forensics training, better equipped cyber cells and clearer procedures for preserving digital evidence would close the enforcement gap identified earlier more effectively than further amendments to the substantive law.

D. STRENGTHENING INTERNATIONAL COOPERATION

[22] The Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).

[23] Indian Computer Emergency Response Team, Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet (Apr. 28, 2022).

Cross border enforcement difficulties call for faster legal assistance mechanisms and stronger cooperation with global technology and payment platforms whose cooperation often determines whether an investigation can be concluded at all.

Taken together these measures target implementation rather than the substance of the law itself the area where this article has located India's most persistent difficulty.

VI. CONCLUSION

India's rapid digital transformation has expanded economic activity, public services and digital commerce but it has not been matched by an equally rapid strengthening of the legal and institutional mechanisms needed to protect individuals, businesses and public institutions from increasingly sophisticated cyber threats. This article demonstrates that India's existing legal framework provides a substantial foundation for addressing cyber security concerns. The Information Technology Act, 2000 together with subsequent legislative and regulatory developments governs a wide range of cyber offences and establishes the institutional mechanisms necessary for responding to cyber incidents. At the same time the analysis reveals that the principal challenge facing India's cyber security framework does not lie in the absence of legal provisions but in the practical difficulties associated with their implementation. The rapidly evolving nature of cyber threats, jurisdictional complexities, institutional capacity constraints and delays in enforcement continue to limit the effectiveness of the existing legal regime.

Strengthening India's cyber security framework therefore requires more than legislative reform alone. Greater coordination between the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, a more operationally effective CERT-In stronger investigative capabilities and enhanced international cooperation are essential to improving cyber resilience. Ultimately, India's cyber security framework is reasonably comprehensive in defining prohibited conduct its continuing challenge lies in ensuring that those legal provisions are implemented consistently, enforced effectively and supported by institutions capable of responding to an increasingly complex digital environment.