



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.

CYBERSECURITY LAWS IN INDIA

~Sangita Roy

ABSTRACT

India's rapid digital transformation has created unprecedented opportunities for economic development, governance and social interaction. At the same time, increasing dependence on digital systems has exposed individuals, businesses and public institutions to cyberattacks, identity theft, ransomware, data breaches, cyber fraud and threats to critical infrastructure. India's response has developed through a combination of the Information Technology Act, 2000, subordinate legislation, institutional mechanisms, criminal law and data-protection regulation. The Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 have further expanded this legal landscape. This article examines the evolution of cybersecurity law in India and argues that the principal difficulty is no longer simply the absence of legislation, but the fragmentation of the existing framework. Effective cybersecurity requires more than criminalizing cyber offences. It requires prevention, incident response, protection of personal information, institutional coordination, accountability and respect for constitutional rights. The article therefore argues for a shift from a predominantly reactive approach towards a resilient and rights-conscious cybersecurity framework.

INTRODUCTION

Digital technology has become an essential part of everyday life in India. Banking, education, healthcare, commerce, communication and public administration increasingly depend upon digital networks. The expansion of digital payments and online public services has made technology an important part of India's economic and social infrastructure. However, greater dependence also creates greater vulnerability. A cyberattack against a digital system can result in financial loss, exposure of personal information, interruption of essential services and, in serious circumstances, consequences for national security.

Cybersecurity should therefore not be viewed merely as a technical problem. It is also a legal problem because the law determines what conduct is prohibited, who is responsible for protecting information, when the State may intervene, how cyber incidents must be reported and what remedies are available to affected persons.

India does not presently regulate cybersecurity through one comprehensive cybersecurity statute. Instead, its framework consists of the Information Technology Act, 2000 (“IT Act”), rules framed under it, institutional mechanisms such as the Indian Computer Emergency Response Team (“CERT-In”) and the National Critical Information Infrastructure Protection Centre (“NCIIPC”), intermediary regulation, general criminal law and data-protection legislation. The Digital Personal Data Protection Act, 2023 (“DPDP Act”) and the Digital Personal Data Protection Rules, 2025 have added another significant layer to this framework¹.

This raises an important question: **Has India developed a comprehensive cybersecurity framework, or has it merely accumulated laws dealing with separate aspects of digital risk?**

The distinction is important because cybersecurity is much broader than cybercrime. Punishing an offender after an attack does not necessarily prevent the attack, protect the victim or restore a compromised system. A meaningful cybersecurity framework must therefore address prevention,

¹ Information Technology Act, No. 21 of 2000, India Code (2000); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

preparedness, incident response, data protection, institutional responsibility and constitutional safeguards.

This article argues that India's cybersecurity regime has developed considerably, but its effectiveness continues to be limited by fragmentation, technological change, institutional capacity and the difficult balance between security and individual rights.

THE INFORMATION TECHNOLOGY ACT, 2000: THE FOUNDATION OF INDIAN CYBER LAW

The IT Act is the foundation of India's statutory response to the digital environment. When enacted in 2000, its principal purpose was to provide legal recognition to electronic records and electronic transactions and facilitate electronic commerce and governance². At that time, the scale and nature of India's digital dependence were very different from the present environment.

The Information Technology (Amendment) Act, 2008 significantly expanded the legislation. It introduced provisions dealing with identity theft, cheating by personation through computer resources, violation of privacy and cyber terrorism³. Section 43 creates civil liability for several unauthorized acts involving computer systems, including unauthorized access, downloading or extraction of data and disruption of computer resources⁴. Section 66 provides criminal liability where specified acts under section 43 are committed dishonestly or fraudulently⁵. Sections 66C and 66D address identity theft and cheating by personation using computer resources or communication devices⁶. Section 66E deals with violation of privacy, while section 66F addresses cyber terrorism⁷. These provisions demonstrate that the IT Act does not treat every cyber incident as identical. An individual's stolen credentials, a fraudulent online transaction and an attack threatening national security may require different legal responses.

² Information Technology Act, No. 21 of 2000, pmbl., India Code (2000).

³ Information Technology (Amendment) Act, No. 10 of 2009, India Code (2009).

⁴ Information Technology Act, No. 21 of 2000, § 43, India Code (2000).

⁵ Id. 66

⁶ Id. 66C-66D

⁷ Id. 66E-66F

Nevertheless, the principal limitation of the IT Act is that it was developed in a technological environment substantially different from today's. Artificial intelligence, cloud computing, sophisticated ransomware, interconnected devices and large-scale data ecosystems present risks that could not have been fully anticipated in 2000.

The answer, however, should not simply be the continuous creation of new offences. An excessively fragmented criminal framework may create uncertainty. What is required is clearer coordination between the IT Act, data-protection legislation and general criminal law.

FROM PUNISHMENT TO PREVENTION: THE ROLE OF CERT-IN

One of the most important developments in India's cybersecurity framework is the recognition that cybersecurity cannot depend entirely upon criminal prosecution. Section 70B of the IT Act establishes CERT-In as the national agency responsible for responding to computer-security incidents⁸. Its functions include collecting and analyzing information concerning cyber incidents, issuing alerts and advisories and coordinating responses. This represents a shift from a purely reactive legal model. If the State waits until an attack has caused substantial damage before responding, the law may punish the offender but may not prevent the harm. Cybersecurity therefore requires early detection and coordinated incident response.

CERT-In's Directions of April 28, 2022 provide an important example. Issued under section 70B, the Directions require specified entities to report listed cyber incidents to CERT-In within six hours of noticing them or being informed about them⁹. They also address logging, time synchronization and the furnishing of information required for incident analysis¹⁰. The reporting requirement has a legitimate objective: a cyber incident affecting one organization may provide information capable of protecting other organizations. Nevertheless, mandatory reporting must be implemented carefully. The better approach is one that combines accountability with assistance. Reporting should strengthen national cybersecurity rather than merely create another regulatory burden

⁸ Id. 70B

⁹ Indian Computer Emergency Response Team, Directions Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet (Apr. 28, 2022).

¹⁰ Id.

CRITICAL INFORMATION INFRASTRUCTURE AND NATIONAL SECURITY

The IT Act recognizes this through its provisions concerning protected systems and critical information infrastructure. Section 70 permits certain computer resources to be declared protected systems, while section 70A provides for a national nodal agency for the protection of critical information infrastructure¹¹. NCIIPC performs specialized functions in this field.

The importance of critical infrastructure protection has increased as sectors such as banking, telecommunications, energy, transport and public administration become increasingly dependent upon interconnected digital systems. A major difficulty, however, is that critical infrastructure is not necessarily controlled exclusively by the State. Private entities may operate systems that are economically or socially essential. Cybersecurity therefore requires cooperation between government authorities and private operators.

Such cooperation must be accompanied by clear responsibility. Organizations operating critical systems should not be able to avoid responsibility by treating cybersecurity solely as a governmental concern. At the same time, governmental authorities should not use the language of national security to justify unlimited access to private or commercially sensitive information.

CYBERSECURITY AND THE RIGHT TO PRIVACY

Perhaps the most difficult legal question arises when cybersecurity measures require access to information about individuals. Section 69 of the IT Act permits interception, monitoring or decryption of information in specified circumstances¹². Section 69A separately provides a statutory framework for blocking public access to information through computer resources.

These powers operate within a constitutional environment that has changed substantially since the enactment of the IT Act. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognized privacy as a constitutionally protected right¹³. Privacy was understood not merely as

¹¹ Information Technology Act, No. 21 of 2000, §§ 70, 70A, India Code (2000).

¹² Id. § 69.

¹³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

secrecy but as an aspect of dignity, autonomy and personal liberty. This constitutional development has significant implications for cybersecurity. The State has a legitimate interest in protecting national security and investigating cyber threats, but the existence of such an interest does not automatically justify every form of surveillance.

Cybersecurity measures involving personal information must therefore be assessed through principles of legality, legitimate purpose, necessity and proportionality. Security cannot become a justification for unrestricted surveillance. At the same time, privacy and cybersecurity should not be treated as opposite objectives. A secure system protects privacy by preventing unauthorized access to personal information. Privacy safeguards, in turn, ensure that security mechanisms themselves do not become sources of abuse.

The stronger approach is therefore to treat privacy and cybersecurity as mutually reinforcing components of digital trust.

SHREYA SINGHAL AND THE LIMITS OF ONLINE REGULATION

The Supreme Court's decision in *Shreya Singhal v. Union of India* is central to understanding the constitutional limits of cyber regulation. The Court struck down section 66A of the IT Act for violating freedom of speech under Article 19(1)(a) of the Constitution¹⁴.

The decision is significant beyond the specific provision that was challenged. It demonstrates that the digital environment does not exist outside constitutional protection. The State may regulate genuinely harmful conduct, but the mere fact that an activity occurs online does not remove constitutional limitations. Cybersecurity legislation must therefore distinguish between unlawful conduct and legitimate digital expression.

This principle becomes increasingly relevant as India regulates social-media platforms, online intermediaries and emerging technologies. Security concerns must be addressed through precise and proportionate legal measures rather than broad restrictions capable of affecting lawful speech.

¹⁴ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

THE DPDP ACT, 2023 AND THE SECURITY OF PERSONAL DATA

Cybersecurity cannot be separated from data protection because many cyber incidents ultimately harm individuals through the exposure or misuse of personal information. The DPDP Act creates a statutory framework for the processing of digital personal data and seeks to balance the interests of individuals in protecting their personal data with the need for lawful processing¹⁵. It imposes obligations upon Data Fiduciaries and provides rights to Data Principals within the statutory framework.

The significance of the DPDP Act lies partly in its recognition that data protection is not merely an internal business concern. Organizations handling personal data have legal responsibilities towards the individuals to whom the information relates.

A data breach can cause consequences far beyond the technical compromise of a database. It may facilitate identity theft, financial fraud, impersonation, harassment or long-term loss of control over personal information.

Nevertheless, the DPDP Act should not be regarded as a complete cybersecurity statute. Data protection and cybersecurity overlap, but they are not identical. Cybersecurity also includes the protection of non-personal information, networks, operational systems, critical infrastructure and national-security interest. The DPDP framework should therefore complement rather than replace the broader cybersecurity regime.

THE DPDP RULES, 2025 AND THE EMERGING COMPLIANCE FRAMEWORK

The Digital Personal Data Protection Rules, 2025 were notified in November 2025¹⁶. The Rules provide operational detail for implementation of the DPDP Act and establish a phased commencement structure¹⁷.

¹⁵ Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–10, India Code (2023).

¹⁶ Digital Personal Data Protection Rules, 2025, Gazette of India, Extraordinary, Part II, Sec. 3(i), G.S.R. 846(E) (Nov. 13, 2025).

¹⁷ Id.

For organizations, however, the growing number of cybersecurity and data-protection requirements creates a practical difficulty. Compliance cannot be approached as a matter of merely possessing a privacy policy. Organizations must understand what information they hold, why they process it, how it is secured and what must happen when a security incident occurs.

The legal framework should therefore encourage genuine security practices rather than formal compliance alone. A company may technically possess a cybersecurity policy while remaining highly vulnerable in practice. The effectiveness of the DPDP framework will consequently depend not only upon penalties but upon whether organizations develop a genuine culture of responsible data management.

INTERMEDIARIES AND DIGITAL PLATFORMS

Digital intermediaries occupy a particularly important position in cybersecurity because they connect millions of users and often process enormous quantities of information.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose due-diligence obligations upon intermediaries¹⁸. These obligations reflect the increasing expectation that platforms should take reasonable steps to address unlawful activity and provide mechanisms for grievances.

However, intermediary regulation presents a difficult balance. If platforms bear too little responsibility, victims may have limited remedies. If platforms are exposed to excessively broad liability, they may remove lawful content merely to avoid risk. The objective should therefore be reasonable due diligence, transparency and accountability rather than unrestricted intermediary liability.

The constitutional principles developed in *Shreya Singhal* remain important in ensuring that regulation of digital platforms does not unnecessarily interfere with lawful expression.

¹⁸Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, Extraordinary, Part II, Sec. 3(i) (2021).

CYBERCRIME UNDER THE NEW CRIMINAL LAW FRAMEWORK

Cybercrime does not always fit exclusively within the IT Act. Technology may be used to commit offences that are also recognized under general criminal law.

The Bharatiya Nyaya Sanhita, 2023 (“BNS”) replaced the Indian Penal Code with effect from July 1, 2024¹⁹. The Bharatiya Nagarik Suraksha Sanhita, 2023 (“BNSS”) similarly replaced the Code of Criminal Procedure and provides the contemporary procedural framework for criminal investigation and prosecution²⁰.

This creates an important overlap. An online fraud, for example, may involve provisions of the IT Act as well as general offences under the BNS. Investigators must consequently understand both specialized cyber law and general criminal law.

The problem is not simply statutory interpretation. Cyber investigations frequently involve electronic evidence, digital trails, cloud storage, encryption and cross-border information. Effective enforcement therefore requires specialized training for police officers, prosecutors and judges.

CROSS-BORDER CYBERCRIME: A JURISDICTIONAL PROBLEM

Cybercrime presents a serious challenge to traditional territorial concepts of criminal jurisdiction. An Indian victim may be targeted by an offender located abroad, using infrastructure hosted in a third country and transferring money through accounts maintained in another jurisdiction. The evidence may consequently be distributed across several legal systems.

Domestic legislation can criminalize the conduct, but prosecution may depend upon international cooperation for obtaining evidence, identifying offenders and securing extradition or other legal assistance. India therefore needs continuing development of international cooperation mechanisms

¹⁹ Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).

²⁰ Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, India Code (2023).

relating to electronic evidence and transnational cybercrime. Domestic cybersecurity legislation alone cannot solve a problem that is inherently global.

THE CENTRAL WEAKNESS: FRAGMENTATION

The principal weakness of India's cybersecurity framework is, in my view, fragmentation rather than complete legislative absence. A single cyber incident may simultaneously involve the IT Act, CERT-In requirements, data-protection obligations, intermediary regulation, sectoral rules and general criminal law. Multiple legal instruments are not inherently problematic, but overlapping responsibilities can create uncertainty.

Victims face a similar problem. A person whose personal information has been stolen may not understand whether the appropriate remedy lies through the police, an intermediary, a data-protection mechanism or another regulatory authority.

India therefore requires greater institutional coordination and clearer compliance guidance. The future framework should make responsibility easier to identify rather than simply increasing the number of regulatory requirements.

THE WAY FORWARD: FROM CYBERSECURITY TO DIGITAL RESILIENCE

India's future cybersecurity policy should move from a reactive model towards digital resilience.

First, cybersecurity obligations should be proportionate to the nature and scale of the organization. A large financial institution and a small enterprise do not possess identical resources or face identical risks.

Second, incident reporting should be accompanied by technical assistance and clear procedures. The purpose of reporting should be collective security, not merely punishment.

Third, privacy should be incorporated into cybersecurity planning from the beginning. Organizations should minimize unnecessary collection and retention of personal information while protecting information that must legitimately be retained.

Fourth, law-enforcement agencies require specialized cybersecurity training. Cybercrime cannot be investigated effectively through traditional methods alone.

Fifth, courts and prosecutors require greater familiarity with electronic evidence and emerging technologies. The legal system must understand technical evidence while continuing to protect procedural fairness.

Finally, cybersecurity should be understood as a shared responsibility. Government, private organizations, technology providers and individual users all form part of the digital ecosystem.

CONCLUSION

India's cybersecurity law has developed significantly since the enactment of the Information Technology Act, 2000. The country now possesses statutory provisions addressing cyber offences, institutional mechanisms for incident response, arrangements for protecting critical information infrastructure, intermediary regulation and a dedicated framework for digital personal data. Yet the existence of multiple laws does not automatically produce effective cybersecurity.

The central challenge is to transform these separate legal components into a coherent system capable of preventing attacks, responding quickly when they occur and protecting the rights of those affected. Cybersecurity cannot be reduced to criminal punishment after an incident. It must include preparedness, resilience, institutional accountability and responsible data governance.

The constitutional dimension is equally important. The decisions in *Puttaswamy* and *Shreya Singhal* demonstrate that India's digital future must remain within the framework of constitutional rights. Security is essential, but security itself must operate through law.

The future of Indian cybersecurity law should therefore rest on four interconnected principles: prevention, accountability, privacy and resilience. The objective should not be to create a system in which security overrides liberty, nor one in which privacy prevents legitimate security action. The objective should be to establish a digital environment in which both can coexist.

India's digital transformation is unlikely to slow down. The legal system must consequently do more than respond to the cyber threats of today. It must create principles capable of adapting to the threats of tomorrow while ensuring that technological progress remains consistent with individual dignity, constitutional freedoms and the rule of law.