



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 LAW IN INDIA: OVERVIEW AND RECENT TRENDS

- *Iffat Zehra*

From a simple law on technological facilitation, India's cyber law has grown to a multi-layered system that regulates cybersecurity, data, and digital responsibility. This is all the more important for companies, citizens, and professionals that want to operate within India's digital economy. It is vital to have an idea of the cyber law development and future trends.

A. THE FOUNDATIONAL FRAMEWORK:

The Information Technology Act of 2000 (IT Act) is the primary legal authority designed to provide legal grounds for digital signatures and electronic commerce, besides giving effect to criminalizing offenses such as identity theft, hacking, and cyberterrorism. Although Section 66 and subsections 66B through 66F of the IT Act 2000 created offenses related to computer fraud, identity theft, and cyberterrorism, Section 43A of the Act, which was introduced by the 2008 amendment (Anon., n.d.), imposed civil liability on enterprises that did not exercise due diligence while handling sensitive personal data. On the other hand, Section 69 of the IT Act 2000 enables the government to monitor, intercept, and decrypt information for the security and sovereign integrity of the country ((India), n.d.).

In the case of *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, the Supreme Court struck down Section 66A of the IT Act, which made "offensive" messages on the Internet illegal, as being unconstitutionally vague and violating the right to free speech under Article 19(1)(a) ((India), n.d.). This was a significant ruling. This decision was cited in subsequent cases concerning the regulation of Internet speech, and has had a profound impact on the jurisprudence of the Indian Internet.

A nine-judge bench recognized the right to privacy as intrinsic to Article 21 in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (*Shreya Singhal v Union of India* ,

2015). This was yet another landmark judgment in the Indian jurisprudence of the Internet and digital rights. As a result of this ruling, any law seeking to restrict informational privacy was required to demonstrate that its restrictions were lawful, necessary, and proportionate. This judgment, therefore, laid the groundwork for subsequent data protection laws in India.

B. THE REGULATORY ECOSYSTEM: CERT-In AND IT RULES:

The Ministry of Electronics and Information Technology regulates Indian Computer Emergency Response Team or CERT-In. It is the mandated authority to handle cybersecurity incidents. The cybersecurity professionals are both worried and supportive of the updated 2022 directions about the reporting mechanism of certain kind of cyber-attacks to be done within six hours of observation (Justice K.S. Puttaswamy (Retd.) v Union of India , 2017).

The guidelines which state the due diligence process like traceability requirements for the top social media companies and a three-tier grievance system for digital media and Over-The-Top or OTT content are mandated by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and subsequent amendments. ((India)., n.d.)

C. THE DPDP ACT: INDIA'S DATA PROTECTION TURNING POINT:

The Digital Personal Data Privacy Act, 2023 (DPDP Act), which not only provides India with a comprehensive data privacy statute for the first time but also replaces the inadequate protections offered by the Section 43A of the IT Act as well as the 2011 SPDI Rules ((India)., n.d.), is by far the most recent and revolutionary development. The previous statutes, which outlined only a few safeguards and failed to consider the rapid emergence of digital technologies, were the main sources of obligation for data protection before the advent of new laws.

On 13th November 2025, The Ministry of Electronics and Information Technology issued the Digital Personal Data Protection Rules, 2025, which allows companies eighteen months to revise systems, procedures, and organizational structures concerning IT, legal, human resources, marketing, and vendors ((India)., n.d.). The Telecom Disputes Settlement and Appellate Tribunal hears appeals from the Data Protection Board of India, which was constituted by the Act to oversee compliance, probe complaints, and levy penalties. Data principals may now exercise their rights freely, including object to processing, data portability,

access to data, correction, or erasure of personal data, and right to be informed about the processing purpose.

By 2026, active enforcement will have overtaken the period of grace for implementation. More stringent data protection norms, including a significantly expanded Significant Data Fiduciaries list encompassing mid-sized (Anon., 2026) fintech, healthtech, and edtech companies, mandatory, time-bound breach notifications to the Data Protection Board and affected individuals, and enhanced coordination mechanisms between CERT-In and the Board for simultaneous incident response and investigations, are also vital elements. The DPDP enforcement and the Data Protection Board's activation from late 2025 have made cybersecurity a board-level priority, transforming it from a purely technical IT responsibility. (Chambers and Partners (2026) Cybersecurity 2026, 2026)

D. EMERGING THREATS AND THE AI GOVERNANCE GAP:

Currently, the situation with the security environment is extremely tense. In 2025, India was confronted with record-breaking cybersecurity threats in the form of attacks on critical infrastructure associated with geopolitical issues and AI-powered deepfake fraud, which is said to have cost the state INR 70,000 crore (Anon., 2026). The judiciary and government are greatly concerned about digital-based arrest scams, with fraudsters posing as police officers and demanding victims pay them.

A unique regulatory issue is raised by artificial intelligence. While the DPDP Act does not directly control AI, it does regulate the collection, storage, and dissemination of information that may be used by firms, including those utilizing AI methods. As a result, companies are responsible for the effects of their AI processing, whether they build the technology themselves or buy it from a third party. Moreover, authors foresee a shift in the future that will fill the legislative lacuna left by India's overall strategy for regulating AI, which primarily takes the form of policy precepts rather than enforceable legal rules. (Anon., 2026)

E. CONCLUSION:

From a facilitative IT statute to a rights based data protection regime with an active regulator, Indian cyber law has come a long way. However, the rate of technological advancement, particularly with respect to AI-enabled fraud and deepfake, far exceeds legislative reactions. The enforcement mechanism of the DPDP Act as well as CERT-In's incident response structure

will probably be tested in the coming years to ensure that it can keep up with innovation while protecting Indian cyberspace.

F. REFERENCES:

1. Information Technology Act 2000 (India).
2. Digital Personal Data Protection Act 2023 (India).
3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India).
4. Shreya Singhal v Union of India (2015) 5 SCC 1.
5. Justice K.S. Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1.
6. Chambers and Partners (2026) Cybersecurity 2026, <https://practiceguides.chambers.com/practice-guides/cybersecurity-2026/india/> (last accessed on 27 September 2026).
7. Chambers and Partners (2026) Data Protection & Privacy 2026 Trends and Developments., <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2026/india/trends-and-developments> (last accessed on 27 September 2026).
8. Fortra (2026) What Is India's Digital Personal Data Protection Act? ,<https://www.fortra.com/blog/what-indias-digital-personal-data-protection-act> (last accessed on 27 September 2026).
9. The Cyber Express (2025) India's DPDP Act: Why 2026 Is the Year Privacy Becomes Real. <https://thecyberexpress.com/india-dpdp-act-will-change-data-handling-2026/> (last accessed on 27 September 2026).
10. SISA (2025) Data Protection and Privacy Acts in India: A 2026 Guide. <https://sisa.ai/resource/blog/data-protection-and-privacy-laws-in-india-2025> (last accessed on 27 September 2026).