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

CYBER LAW IN INDIA: OVERVIEW AND RECENT TRENDS

~ Sanskriti Mishra

INTRODUCTION

The rapid expansion of digital technology has fundamentally transformed the social, economic, and legal landscape of India. The growth of internet accessibility, digital payment systems, artificial intelligence, cloud computing, e-commerce, and social media platforms has accelerated India's transition toward a digital economy. Government initiatives such as Digital India and the increasing dependence on online services have further contributed to this transformation. However, the growth of cyberspace has simultaneously resulted in the rise of cybercrimes including hacking, phishing, cyberstalking, identity theft, ransomware attacks, financial frauds, and data breaches.

The increasing complexity of cyber threats has made cyber law an indispensable aspect of modern legal governance. Cyber law refers to the body of laws governing activities conducted through computers, digital networks, and electronic communication systems. In India, the primary legislation-regulating cyberspace is the IT Act, which provides legal recognition to electronic transactions and establishes punishments for cyber offences.

Recent developments such as the implementation of the DPDP Act, 2023 and the operationalization of the DPDP Rules, 2025 reflect India's evolving approach toward data privacy and cybersecurity regulation. India's growing digital ecosystem has therefore necessitated a stronger legal framework capable of balancing innovation, privacy, cybersecurity, and freedom of expression.

MEANING AND SCOPE OF CYBER LAW

Cyber law refers to the legal framework regulating the use of computers, digital devices, cyberspace, and the internet. It governs legal issues arising from electronic communication, digital transactions, online conduct, and information technology systems. Cyber law encompasses several areas including cybercrime regulation, e-commerce, data protection, digital governance, intellectual property rights, and intermediary liability.

The scope of cyber law is extremely broad. It regulates electronic contracts and digital signatures, facilitates e-commerce transactions, protects confidential data, and establishes liability for cyber

offences. Cyber law also governs the responsibilities of intermediaries such as social media platforms and online service providers.

The importance of cyber law has increased significantly due to the rapid digitization of financial systems and governance mechanisms. The absence of effective cyber regulation can lead to severe threats to individual privacy, national security, and economic stability. Consequently, cyber law plays a critical role in ensuring legal certainty and cybersecurity in the digital era.

LEGAL FRAMEWORK GOVERNING CYBER LAW IN INDIA

Information Technology Act, 2000

The IT Act is the primary legislation governing cyber law in India. The Act was enacted to provide legal recognition to electronic records and digital signatures while facilitating electronic commerce and e-governance. The Act criminalizes several cyber offences including hacking, identity theft, cyber terrorism, and publication of obscene material in electronic form. It also establishes adjudicatory mechanisms and prescribes penalties for unauthorized access to computer systems.

The IT Act was heavily influenced by the UNCITRAL Model Law on Electronic Commerce and represented India's first comprehensive attempt to regulate cyberspace.

Information Technology (Amendment) Act, 2008

The Information Technology (Amendment) Act, 2008 introduced major reforms to address emerging cyber threats. The amendment expanded the scope of cyber offences and introduced provisions relating to identity theft, violation of privacy, cheating by personation, and cyber terrorism.

One of the significant additions under the amendment was Section 66A, which criminalized offensive online communication. However, the Supreme Court in *Shreya Singhal v. Union of India* later declared the provision unconstitutional because of its vague and arbitrary nature. The amendment also introduced intermediary liability provisions under Section 79, granting conditional immunity to online intermediaries subject to due diligence requirements.

Digital Personal Data Protection Act, 2023

The enactment of the Digital Personal Data Protection Act, 2023 ("DPDP Act") marked a major development in India's data privacy regime. The legislation establishes a framework governing the processing of digital personal data and seeks to balance individual privacy rights with lawful data processing requirements.

The Act introduces several important concepts including:

- consent-based processing,
- rights of data principals,
- obligations of data fiduciaries,

- data breach reporting requirements, and
- Monetary penalties for non-compliance.

The implementation of the DPDP Rules, 2025 operationalized India's first comprehensive digital privacy framework and introduced phased compliance obligations for organizations handling personal data.

Recent reports indicate that the Rules require companies to strengthen consent mechanisms, data retention policies, breach notification procedures, and user privacy protections.

IMPORTANT PROVISIONS UNDER CYBER LAWS

Section 43 – Penalty for Damage to Computer Systems

Section 43 of the IT Act imposes civil liability for unauthorized access, downloading of confidential information, introduction of viruses, and disruption of computer systems.

Section 66 – Computer Related Offences

Section 66 criminalizes acts mentioned under Section 43 when committed dishonestly or fraudulently. The provision primarily addresses hacking and unauthorized access to digital systems.

Section 66C – Identity Theft

Section 66C punishes fraudulent use of passwords, electronic signatures, or digital identities. The increasing use of digital payment systems has led to a rise in identity theft cases across India.

Section 66D – Cheating by Personation

Section 66D criminalizes cheating by personation through digital means including phishing scams and online financial frauds.

Section 67 – Obscene Material in Electronic Form

Section 67 punishes the publication or transmission of obscene content in electronic form and seeks to regulate unlawful online material.

Section 69 – Government Surveillance Powers

Section 69 empowers the Government to intercept, monitor, or decrypt digital information in the interest of national security and public order. However, concerns regarding excessive surveillance and misuse of such powers continue to generate constitutional debates relating to privacy rights.

RECENT TRENDS AND DEVELOPMENTS

Rise in Cybercrime Cases

India has witnessed a significant increase in cybercrime incidents due to growing internet penetration and digital transactions. Cybercriminals frequently target banking systems, e-commerce platforms, and social media users through phishing attacks, malware, and ransomware schemes.

The increasing use of artificial intelligence has further complicated cybercrime investigations because AI technologies can now generate sophisticated phishing attacks, deepfakes, and misinformation campaigns.

Data Privacy and DPDP Rules, 2025

One of the most significant recent developments in cyber law has been the operationalization of the DPDP Rules, 2025. The Rules establish a citizen-centric framework focused on consent, accountability, and responsible data processing.

The Rules require organizations to:

- provide clear consent notices,
- establish grievance redressal mechanisms,
- notify users regarding data breaches,
- implement data retention limitations, and
- Strengthen cybersecurity safeguards.

The implementation of these rules demonstrates India's attempt to align its privacy framework with global standards such as the European Union's GDPR.

Artificial Intelligence and Deepfakes

Artificial intelligence has emerged as a major challenge for cyber law enforcement. AI-generated deepfake videos and manipulated digital content raise concerns regarding misinformation, privacy violations, and electoral manipulation.

Current cyber laws in India remain insufficient to comprehensively regulate AI-driven cyber offences. Consequently, there is growing demand for a specialized legal framework governing artificial intelligence and algorithmic accountability.

Increased Regulation of Social Media Platforms

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 introduced stricter obligations for social media intermediaries operating in India. Platforms are now required to establish grievance mechanisms, remove unlawful content, and cooperate with law enforcement authorities.

The increasing regulation of social media platforms reflects growing governmental concerns regarding hate speech, fake news, online abuse, and digital misinformation.

CHALLENGES IN CYBER LAW ENFORCEMENT

Despite legislative progress, cyber law enforcement in India continues to face several challenges.

First, cybercrimes often involve cross-border elements, making investigation and prosecution difficult. Jurisdictional complexities create significant obstacles for law enforcement agencies.

Second, technological advancement evolves faster than legislation. Emerging technologies such as block chain, cryptocurrency, and artificial intelligence frequently expose gaps within existing cyber laws.

Third, a substantial portion of the population remains unaware of cybersecurity practices and legal remedies available under cyber laws. This lack of awareness increases vulnerability to cyber frauds and scams.

Finally, balancing privacy rights with national security concerns remains one of the most controversial issues in cyber jurisprudence. Government surveillance powers under the IT Act have repeatedly generated constitutional debates regarding proportionality and privacy.

LANDMARK JUDICIAL DECISIONS

Shreya Singhal v. Union of India

In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the IT Act on the ground that it violated the fundamental right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution. The Court held that vague expressions such as “grossly offensive” and “annoying” lacked clear legal standards. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

Justice K.S. Puttaswamy v. Union of India

In *Justice K.S. Puttaswamy v. Union of India*, the Supreme Court recognized the Right to Privacy as a fundamental right under Article 21 of the Constitution. The judgment significantly influenced India’s data protection framework and laid the constitutional foundation for privacy legislation. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

Avnish Bajaj v. State (NCT of Delhi)

The Delhi High Court in *Avnish Bajaj v. State (NCT of Delhi)* examined intermediary liability concerning objectionable online content. The case remains significant in determining the liability of online platforms under Indian cyber law. *Avnish Bajaj v. State (NCT of Delhi)*, 150 (2008) DLT 769.

CONCLUSION

Cyber law has become one of the most important areas of legal governance in the digital era. India's rapid technological advancement and increasing dependence on digital systems have created both opportunities and cybersecurity challenges. The Information Technology Act, 2000, along with the Digital Personal Data Protection Act, 2023 and the DPDP Rules, 2025, represents India's evolving approach toward cybersecurity and data protection.

Judicial decisions such as *Shreya Singhal* and *Puttaswamy* have further strengthened constitutional protections relating to freedom of speech and privacy in cyberspace. However, challenges relating to enforcement, jurisdiction, artificial intelligence, and digital surveillance continue to persist.

Therefore, India must continue strengthening its cyber law framework through legislative reforms, technological preparedness, cybersecurity awareness, and international cooperation in order to effectively address emerging digital threats in the modern era.