



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

– Mahipal Yagati



Introduction

The Cyber Law became more important after the Global pandemic "Covid 19" took place. The last time you used UPI for food services through Instagram or Facebook, or received an OTP on your phone, should serve as your starting point for evaluation. The electronic data created by these digital actions included information about your identity, your daily activities, your physical whereabouts and your personal choices. The total number of internet users in India, estimated at 700 million users,¹ demonstrates why cyber law has developed into a critical legal field that requires urgent attention in the country.

India has the data. The real question is: does it have the law to protect it?

Cyber law functions as the legal system that regulates both human behaviour and digital communication methods within online spaces. The law addresses various aspects, including data protection and online business operations, cybercrime activities, digital contractual agreements,

¹ Internet & Mobile Ass'n of India, *India Internet Report 2023* 12 (2023).

intermediary responsibility and numerous other issues. Cyber Law used to be an optional subject, but it has now become a mandatory requirement because of its critical importance, which emerged with new AI technologies and digital security threats.

The Legal Foundation: The IT Act,2000

India's cyber law journey began with the Information Technology Act,2000(IT Act),² which provides legal recognition to electronic records and digital signatures in line with the UNCITRAL Model Law on Electronic Commerce.³ The IT Act created the first framework of civil and criminal liability for digital offences. Section 43 imposed civil liability for unauthorised access to computer systems and data theft.⁴Section 66 criminalised hacking- the dishonest or fraudulent act of securing access to a computer, computer system or computer network⁵. Section 67 penalised the publication of obscene material in electronic form.⁶ And Section 69 empowered the Central Government to intercept, monitor, or decrypt electronic information in the interest of national security.⁷

The **IT (Amendment) Act, 2008**⁸ substantially strengthened this framework by introducing a series of new offences reflecting the evolving threat landscape: Section 66C penalised identity theft,⁹Section 66D addressed cheating by personation using computer resources,¹⁰ Section 66E penalised violation of privacy through capturing, publishing, or transmitting images of a private area without consent,¹¹ and Section 66F — the most serious of all — introduced the offence of cyber terrorism, punishable with imprisonment for life.¹²

A 2000-era statute was never built for the age of artificial intelligence, deepfakes, and real-time data harvesting. Something more was needed.

The Constitutional Backbone: Privacy as a Fundamental Right

The Supreme Court brought about the biggest changes to India's cyber law system through its legal ruling, which The Supreme Court brought about the biggest changes to India's cyber law system through its legal ruling which in K.S. Puttaswamy v. Union of India¹³ established this permanent change. The Supreme Court of India made a historical ruling when its nine-judge Constitution

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

³ U.N. Comm'n on Int'l Trade Law, *UNCITRAL Model Law on Electronic Commerce* (1996), https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce.

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

⁵ *Id.* § 66.

⁶ *Id.* § 67.

⁷ *Id.* § 69; *see also* Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).

⁸ Information Technology (Amendment) Act, No. 10 of 2009 (India).

⁹ *Id.* § 66C.

¹⁰ *Id.* § 66D.

¹¹ *Id.* § 66E.

¹² *Id.* § 66F.

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

Bench ruled on *K.S. Puttaswamy v. Union of India*, which overthrew previous court rulings that protected individual privacy rights through *M.P. Sharma v. Satish Chandra*¹⁴ and *Kharak Singh v. State of Uttar Pradesh*.¹⁵ The Court established that people possess the right to control their personal information, which they share with others. The Court established that any breach of someone's right to control their personal information needs to show three things, which include lawful reasons, proper objectives and balanced methods of execution.

Justice D.Y. Chandrachud (as he then was) observed that the State must establish a strong data protection system which will control how both government entities and private organisations handle personal data.¹⁶ This judicial directive set the stage for the legislative developments that followed.

The DPDP Act, 2023: India's Data Protection Moment

The Digital Personal Data Protection Act, 2023 (DPDP Act),¹⁶ which received Presidential assent on 11 August 2023, became India's first law to address digital personal data security. The law serves as the first complete Indian legal framework for protecting personal data. The DPDP Act¹⁷ establishes a consent-based framework that requires Data Fiduciaries to obtain free informed specific consent from Data Principals before they process personal data. Data Principals receive important rights through this law, which include their right to access data about themselves (Section 11), their right to request data correction and deletion (Section 12), their right to file complaints (Section 13), and their right to assign someone else to represent them after their death or disability (Section 14). Section 9 requires verifiable parental consent for processing children's data while it bans all forms of behavioural tracking and targeted marketing towards minors.

Enforcement rests with the **Data Protection Board of India**, established under Sections 18 to 27 of the Act,¹⁸ which can impose financial penalties of up to Rs. 250 crore for breaches involving children's data and up to Rs. 200 crore for failure to implement adequate security safeguards.

Recent Regulatory Trends

Upcoming regulatory changes that will impact business operations should be monitored closely, as they will emerge as critical developments. The DPDP Act includes multiple important regulatory changes that have transformed the complete framework of Indian cyber laws. The **IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021**¹⁹ established multiple new requirements for social media intermediaries, requiring them to hire Grievance Officers for their Indian operations, to acknowledge incoming complaints within one day, and to process

¹⁴ *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300 (India).

¹⁵ *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295 (India).

¹⁶ Personal Data Protection Bill, No. 373 of 2019 (withdrawn Aug. 3, 2022) (India).

¹⁷ Digital Personal Data Protection Act, No. 22 of 2023 (India).

¹⁸ *Id.* §§ 18–27.

¹⁹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

takedown requests within fifteen days. The first time, large platforms now bear actual responsibility for the material that they store on their systems.

The emergence of **deepfakes together with AI-generated content**, has created a major empty space in existing regulatory frameworks. The Ministry of Electronics and Information Technology issued an Advisory in November 2023,²⁰ which warned platforms about deepfake distribution and requested them to implement security measures against this threat, yet current laws provide no control over synthetic media creation and distribution. The current situation requires urgent action because social media networks continuously share fake content.

Cyber crimes continue to rise sharply. The National Crime Records Bureau reported in its Crime in India 2022 report that 65893 cybercrime cases occurred throughout India in 2022, which marked a 244 per cent increase from the 52974 cases that happened in 2021.²¹ The highest number of reported crimes included financial fraud, together with online harassment, which demonstrated how digital criminals have developed advanced methods to operate.

The Challenges That Still Remain

Jurisdictional complexity: Determining which laws apply becomes a difficult task when a hacker from one nation breaks into a bank located in another country while operating from servers situated in a third nation. The absence of a complete international treaty system for cross-border cybercrime in India creates obstacles for countries to work together on cybercrime matters. An enforcement gap exists because police stations across the country lack enough trained officers who can handle cybercrime investigations. The combination of victim stigma and limited knowledge about national cybercrime reporting through cybercrime.gov.in creates a situation where actual cybercrime incidents remain unreported. The IT Act and the DPDP Act lack any legal provisions that would regulate automated decision-making and address algorithmic bias and AI system dangers. The current absence of artificial intelligence laws in India creates harmful effects on people's lives because AI systems now control who can receive credit, enter the workforce and access government services.

Why This Matters — For You

²⁰ Ministry of Elecs. & Info. Tech., Gov't of India, Advisory to Platforms Regarding Deepfakes (Nov. 2023).

²¹ Nat'l Crime Records Bureau, *Crime in India 2022*, at ch. 18, tbl. 18.1 (Ministry of Home Affs. 2023).

Cyber law exists as a legal framework that applies to both technology companies and government regulators. The law oversees all digital interactions that people experience from the time they unlock their phones until they complete their electronic signatures. The legal profession offers law students and aspiring practitioners the most dynamic and future-proof career path through this field. India stands at a pivotal moment. The constitutional foundation has been laid by Puttaswamy. The first comprehensive data protection statute is now on the books. The regulatory system develops through its incremental construction method. The system suffers from major deficiencies because of missing AI governance, enforcement systems, international collaboration systems, and complete implementation of the DPDP Act's Rules, which still require official release.

The digital future is being written right now. The lawyers who understand cyber law today will shape how that future is governed tomorrow.

Cyber law provides equal opportunities for data privacy and corporate compliance and cybercrime prosecution, platform regulation, and technology policy. The field is still developing because it presents difficult questions that have critical implications for society. That is exactly why you should spend your time on this.