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: Emerging Issues and Challenges

Yashi Agarwal

Abstract

Technology has become an inseparable part of human life in the modern era. From online banking and digital payments to social media and e-governance, almost every activity today depends upon the internet and computer systems. However, these technological developments have also resulted in a significant increase in cybercrimes, data breaches, identity theft, online fraud, cyberterrorism, and privacy violations. The legal framework governing cyberspace in India is primarily based on the Information Technology Act, 2000, which has undergone amendments to address evolving technological challenges. Emerging technologies such as artificial intelligence, cryptocurrency, blockchain systems, and deepfake technology have further complicated the legal landscape. This research paper examines the concept and evolution of cyber law in India, analyzes the existing legal framework, discusses major emerging issues, and highlights the challenges faced in enforcement. The paper also evaluates the role of the judiciary and suggests reforms required for strengthening cyber governance in India.

Keywords: Cyber Law, Cybercrime, Information Technology Act, Data Protection, Artificial Intelligence, Privacy, Cybersecurity.

Introduction

The twenty-first century has witnessed unprecedented technological advancement. The internet has become an integral component of communication, commerce, governance, education, and entertainment. India's digital transformation, accelerated by initiatives such as Digital India, Unified Payments Interface (UPI), Aadhaar integration, and e-governance programs, has created immense opportunities for economic growth and social development.

However, the increased dependence on digital platforms has also exposed individuals, businesses, and governments to numerous cyber threats.

Cyber law refers to the body of legal principles that regulate activities conducted through computer systems, networks, and the internet. It encompasses issues relating to electronic commerce, cybersecurity, digital evidence, data protection, intellectual property rights, privacy, cybercrimes, and intermediary liability. The emergence of sophisticated cyberattacks, ransomware incidents, identity theft, financial frauds, and data breaches has highlighted the need for a comprehensive legal framework capable of addressing contemporary challenges.

India's cyber law regime is primarily governed by the Information Technology Act, 2000.[1] While the legislation was revolutionary at the time of its enactment, rapid technological developments have created regulatory gaps that require urgent attention. The emergence of artificial intelligence, deepfake technology cryptocurrency-based crimes, and transnational cyber offenses poses serious challenges to the effectiveness of existing laws.

Evolution of cyber law in India

As internet usage and electronic commerce started expanding, the need for legal recognition of online transactions became increasingly important. To address this issue, India enacted the Information Technology Act, 2000, which was largely based on the UNCITRAL Model Law on Electronic Commerce.[2]The Act legally recognized electronic records and digital signatures, thereby encouraging e-commerce and online communication. Later, the Information Technology (Amendment) Act, 2008 introduced important provisions relating to cyber terrorism, identity theft, intermediary liability, and data protection.[3] These amendments were introduced to deal with the growing complexity of cybercrimes in India.

Indian courts have also played a major role in shaping cyber law jurisprudence. In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the Information Technology Act because it violated the constitutional right to freedom of speech and expression.[4] This judgment became an important milestone in protecting online free speech in India. Another landmark judgment was *Justice K.S. Puttswamy v. Union of India*, where the

[1] Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
[2] United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162, U.N. Doc. A/RES/51/162 (Dec. 16, 1996).
[3] Information Technology (Amendment) Act, No. 10 of 2009, INDIA CODE (2009).
[4] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

Supreme Court recognized privacy as a fundamental right under the Constitution.[5] This case significantly influenced discussions relating to data protection and informational privacy in the digital era.

Legal Framework Governing Cyber Law in India

Information Technology Act, 2000

The Information Technology Act, 2000 is the primary legislation governing cyber activities in India. The Act grants legal recognition to electronic records and digital signatures, thereby enabling online transactions and electronic communication. The Act also criminalizes several cyber offenses. Sections 43 and 66 deal with unauthorized access to computer systems and hacking activities. Section 66C addresses identity theft, while Section 66D punishes cheating through computer resources. Similarly, Section 67 penalizes the publication of obscene material in electronic form, and Section 66F deals with cyber terrorism.[6] Although the Act was a progressive step at the time of its enactment, many experts believe that it requires modernization to effectively deal with present-day technological challenges.

Digital Personal Data Protection Act, 2023

The enactment of the Digital Personal Data Protection Act, 2023 represents a significant step toward strengthening privacy protection in India. The legislation establishes obligations for data fiduciaries, recognizes the rights of data principals, and prescribes penalties for data breaches.[7] The Act seeks to balance individual privacy rights with legitimate state interests and commercial requirements. Nevertheless, concerns remain regarding implementation mechanisms, exemptions granted to governmental authorities, and enforcement effectiveness.

Indian Penal Code and Bharatiya Nyaya Sanhita

Traditional criminal laws continue to supplement cyber regulations. Offenses involving cheating, forgery, criminal intimidation, defamation, and extortion often overlap with cybercrimes. Consequently, provisions of criminal law operate alongside the IT Act to prosecute cyber offenders.

EMERGING ISSUES IN CYBER LAW

[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[6] Information Technology Act, No. 21 of 2000, §§ 43, 66, 66C, 66D, 66F, 67 (India).
[7] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

Data Privacy and Data Breaches

In today's digital world, personal information has become extremely valuable. Social media platforms, banks, online applications, and e-commerce companies regularly collect large amounts of user data. However, weak cybersecurity systems often result in data breaches and misuse of personal information. In India, concerns regarding surveillance, data misuse, and unauthorized sharing of personal information have increased significantly in recent years.[8] Many people remain unaware of how their information is collected and used online.

Artificial Intelligence and Deepfake Technology

Artificial intelligence has revolutionized multiple sectors including healthcare, education, finance, and law enforcement. However, AI-generated content, deepfake videos, and automated cyberattacks have created novel legal challenges. Deepfake technology enables the creation of realistic but fabricated audio and video content. Such content can be misused for political manipulation, financial fraud, defamation, and cyber harassment. Existing legal provisions are often inadequate to address the complexities associated with AI-generated harms.[9]The absence of a dedicated AI regulatory framework in India creates uncertainty regarding liability, accountability, and ethical governance.

Cyber Financial Frauds

The expansion of digital payment systems has increased exposure to cyber-enabled financial crimes. Phishing attacks, UPI frauds, online banking scams, and cryptocurrency-related offenses have become increasingly common. Cybercriminals exploit social engineering techniques to obtain sensitive financial information from unsuspecting users. Reports indicate substantial financial losses resulting from cyber frauds across various Indian states. The rapid evolution of fraud techniques often outpaces regulatory and investigative capabilities.

Cyber Terrorism and National Security

Cyber-attacks targeting critical infrastructure pose significant risks to national security. Government networks, financial institutions, healthcare systems, and energy grids are increasingly vulnerable to sophisticated cyber intrusions. Cyber terrorism involves the use of computer systems to threaten national security, public order, or critical infrastructure. Section

[8] Deepti Lata & RajVardhan, An Analytical Study of Cyber Law and Legal Framework in India, 11 INT'L J. INNOVATIVE RSCH. ENG'G & MULTIDISCIPLINARY PHYSICAL SCI. 45, 49–52 (2025).
[9] Rs 938 Crore Lost to Cybercrooks Since Jan, Times of India (2025).

66F of the Information Technology Act addresses such offenses; however, attribution difficulties and cross-border operations complicate enforcement efforts.

Challenges in the Enforcement of Cyber Law

Rapid Technological Advancement

One of the biggest challenges in enforcing cyber law is the fast pace of technological development. Technology changes much more quickly than laws can be created or amended. As a result, legal provisions often become outdated before they can effectively deal with newly emerging technologies and cyber threats.The Information Technology Act, 2000, even after the 2008 amendments, still struggles to regulate modern technological issues such as blockchain systems, cryptocurrency-related crimes, artificial intelligence-based attacks, and Internet of Things (IoT) devices.[10]Since cybercriminals continuously adopt new techniques, lawmakers and enforcement agencies often find it difficult to keep up with the changing nature of cyber offenses.

Lack of Specialized Expertise

Another major challenge in cyber law enforcement is the shortage of technical expertise among investigating agencies. Cybercrime investigations require advanced knowledge of cybersecurity, digital forensics, electronic evidence collection, and data analysis. However, many law enforcement agencies in India still face resource limitations and lack adequately trained professionals.In many cases, investigators may not possess the technical skills necessary to properly handle complex cybercrime cases. This affects the quality of investigation and lowers the chances of successful prosecution. Therefore, regular training programs and capacity-building initiatives are essential for police officers, prosecutors, and judges dealing with cyber-related matters.

Digital Evidence and Admissibility

Cybercrime cases mainly depend upon digital evidence such as emails, electronic records, online chats, IP addresses, CCTV footage, and computer data. However, maintaining the authenticity and reliability of such evidence is often difficult.Unlike physical evidence, electronic evidence can be easily altered, deleted, copied, or manipulated without leaving visible traces. Because of this, maintaining proper chain-of-custody procedures becomes

[10] Ahmad Muhammad Tahir, *The Efficacy of the Information Technology Act, 2000, in Addressing Emerging Cyber Threats in India*, 14 INT'L J. SCI. & RSCH. 88, 92–95 (2025).

extremely important during investigations. Courts also require strict compliance with legal rules relating to admissibility of electronic evidence.

Low Reporting and Public Awareness

Many cybercrime cases in India remain unreported. Many victims hesitate to approach authorities because of lack of awareness, fear of social embarrassment, or concerns regarding lengthy legal procedures. In some situations, victims are unaware that they have become targets of cyber fraud or identity theft. Underreporting weakens the effectiveness of cyber law enforcement because authorities are unable to accurately measure the scale of cybercrime. Public awareness campaigns, digital literacy programs, and simplified complaint mechanisms can help encourage timely reporting of cyber offenses.

International Cooperation

Cybercrimes frequently involve cross-border operations, making international cooperation extremely important. A cybercriminal may operate from one country while targeting victims located in another country. This creates serious jurisdictional and procedural difficulties during investigation and prosecution. Differences in national laws, extradition procedures, and evidence-sharing mechanisms often delay cybercrime investigations. Therefore, stronger international cooperation and global cybersecurity agreements are necessary to effectively combat transnational cyber offenses.

Challenges in Enforcement of Cyber Law

One of the biggest problems in cyber law enforcement is the rapid pace of technological advancement. Laws often become outdated because technology changes faster than legislation. The Information Technology Act, despite amendments, struggles to address modern technologies such as blockchain systems, cryptocurrency-related crimes, and AI-driven cyberattacks.[11] Another major challenge is the lack of technical expertise among investigating agencies. Cybercrime investigations require specialized skills in digital forensics, cybersecurity, and electronic evidence collection. Many law enforcement agencies still face shortages of trained professionals and technological resources. Jurisdictional issues also complicate cybercrime investigations. Since cyber offenses can occur across multiple countries simultaneously, determining legal jurisdiction and obtaining international

[11] Ahmad Muhammad Tahir, *The Efficacy of the Information Technology Act, 2000, in Addressing Emerging Cyber Threats in India*, Int'l J. Sci. & Rsch. (2025).

cooperation becomes difficult. In addition, many cybercrime victims hesitate to report incidents due to fear, social stigma, or lack of awareness. This results in underreporting and weak enforcement.

Conclusion

Cyber law has become one of the most important areas of law in the modern digital age. As India continues to move toward a technology-driven economy, the use of the internet and digital platforms has increased rapidly in almost every field, including banking, education, healthcare, communication, governance, and business. While technological advancement has made life more convenient and efficient, it has also created serious risks such as cybercrimes, online frauds, identity theft, hacking, data breaches, cyber terrorism, and privacy violations. The Information Technology Act, 2000 laid the foundation for regulating cyberspace in India and played a significant role in giving legal recognition to electronic transactions and digital communication.[12] Over time, amendments and judicial decisions have further strengthened the cyber law framework. Landmark judgments such as *Shreya Singhal v. Union of India* and *Justice K.S. Puttaswamy v. Union of India* have emphasized the importance of freedom of speech and privacy rights in the digital environment. However, despite these developments, the existing legal framework still faces several challenges in effectively dealing with modern cyber threats.

One of the biggest concerns is that technology evolves much faster than legislation. New technologies such as artificial intelligence, blockchain systems, cryptocurrency platforms, and deepfake technology have created legal and ethical issues that were not fully anticipated when the Information Technology Act was enacted. Cybercriminals constantly develop new methods to exploit technological loopholes, making enforcement increasingly difficult for authorities. Another major challenge is the lack of technical expertise and infrastructure required for effective cybercrime investigation. Many law enforcement agencies continue to face shortages of trained professionals, digital forensic resources, and cybersecurity tools. In addition, jurisdictional issues and cross-border cybercrimes further complicate investigation and prosecution processes. Public awareness regarding cyber safety also remains limited, resulting in underreporting of cyber offenses.

[12] Information Technology Act, No. 21 of 2000, INDIA CODE (2000).

Therefore, there is an urgent need for continuous reforms in India's cyber law framework. Existing laws must be regularly updated according to changing technological realities. Strong cybersecurity policies, stricter data protection mechanisms, international cooperation, digital literacy programs, and specialized cybercrime investigation units are necessary for ensuring a secure digital environment.In conclusion, cyber law will continue to play a crucial role in protecting individuals, businesses, and governments in the digital era. A balanced legal framework that encourages technological innovation while safeguarding privacy, security, and constitutional rights is essential for the future growth of India's digital economy. Effective implementation of cyber laws, combined with public awareness and technological preparedness, will help India address emerging cyber challenges more efficiently and build a safer cyberspace for society.