



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 Laws in India: Emerging Issues and Challenges

(Manasvi Katiyar)

Abstract-

In this technology-driven world, we have seen the rapid growth of technology and increase in the number of cyber related crimes. Incidents like online fraud, identity theft, deepfakes is increasing day-by-day and it is important to stop these and this can only be done when there are strict laws. To tackle these problems, The Information Technology Act of 2000 came into force with an objective to prevent cybercrime and punish cyber criminals. Over the passage of time, amendment in the Information Technology Act, DPDP Act, CERT-in Guidelines have strengthened the cyber regulatory framework.

This research paper deals with the regulatory framework governing cyber laws in India, offences and penalties, case laws. Further, we will also discussed about the emerging issues and challenges. In the conclusion, we will discussed about some of the reforms and recommendations.

Keywords-

Cyber Law, Information Technology Act of 2000, Digital Personal Data Protection Act of 2023, Cybercrime, CERT-In Guidelines

Introduction-

The growing use of internet has given rise to a new area of law known as “Cyber Law”. Cyber Law is also known as Internet law or digital law. Cyber Laws are the laws which deals with internet related technologies such as cyber security, online fraud, online harassments, digital frauds, crypto currency frauds etc. With the increase of technology and internet, cybercrime is also increasing day-by-day. [1]

In India, cyber laws are primarily governed by the Information Technology Act, 2000 which provide basis for regulating electronic record, digital signatures, data protection, and cybercrimes. Subsequent amendment particularly the Information Technology (Amendment) Act, 2008 has broaden the scope of cyber offences such as cyber terrorism, identity theft, and financial frauds. To protect the privacy of the individuals, the Digital Personal Data Protection Act, 2023 was introduced and became a major legislative step for guarding the personal data of the individuals. [2]

Apart from the IT Act, various other laws dealing with the cybercrime in India are-

1. The Indian Penal Code, 1860 (now replaced by The Bhartiya Nyaya Sanhita, 2023),
2. The Indian Evidence Act, 1872 (now replaced by The Bhartiya Sakshya Adhiniyam, 2023),
3. The Information Technology Rules, 2011,
4. National Cyber Security Policy, 2013,
5. Reserve Bank of India Act, 2018 and
6. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. [3]

Methodology-

This study is based on the doctrinal research methodology. This research relies upon the primary sources including acts and policies such as IT Act of 2000, DPDP Act of 2023, Intermediary Guidelines, and cyber security policies. This research also include secondary sources like journals, articles, blogs, and reports. The approach of this paper is descriptive in nature. This research also relies upon the judicial interpretations including case laws. This paper propose suggestive reforms for strengthening India's cyber law framework.

Literature Review-

A wide range of studies shows how India's legal system has attempted to address the challenges posed by the cybercrime and governance of cyber space. Dr. Gupta and Agrawal in their book titled, "Cyber Laws", provide a comprehensive overview of the Indian cyber legal regime, especially focusing on the Information Technology Act, 2000 (IT Act). [4]

K.M. Muralidharan and R. Singaravelan, in their book, titled "Law of Cybercrimes in India", provide a complete analysis of cyber offences, legal procedures, and regulatory framework.

Rohas Nagpal, in his work “Cyber Crime and Corporate Liability”, underscores the emerging threat of corporate cyber liability and explains how insufficient compliance and lack of awareness make Indian corporations vulnerable to cyberattacks and legal sanctions. [4]

Javaid Iqbal and Bilal Manzoor Beigh in his paper titled "Cybercrime in India: Trends and challenges" examines the rapid growth of digital offenses in India, focusing on the legal challenges, prevailing crime trends, and governmental countermeasures. [5]

Laws Governing Cyber Law in India-

1. The Information Technology Act, 2000-

1.1. Overview

- The Information Technology Act, 2000 (hereinafter referred to as the “IT Act”) was enacted by the Parliament of India. It was enacted on 9th June, 2000. The law applies to the whole of India and also include any offence committed outside India by any person. [6]
- The act is based on the principle of Electronic Commerce Model Law adopted by the United Nations Commission on International Trade Law. The act was adopted through the resolution by General Assembly of the United Nations on 30th January, 1997. [6]

1.2.Objective

- The IT Act provide legal recognition for the transactions carried out by means of electronic data and other means of electronic communication. It also provide legal recognition to electronics records and digital signatures. [7]
- The act define various cyber offences and prescribe penalties for their commission. The act also directed a regulatory framework for investigation and adjudication of cybercrimes. [7]

1.3.Provision-

- Section 65- Tampering with the computers source documents.
 - Punishment- Imprisonment up to 3 years or fine up to Rs.2 lakhs or both. [6]
- Section 66- Hacking with computer system.
 - Punishment- Imprisonment up to 3 years or fine up to Rs.2 lakhs or both. [6]

- Section 66B- Dishonestly receiving stolen computer resource or communication device.
 - Punishment- Imprisonment up to 3 years or fine up to Rs.1 lakhs or both. [6]
- Section 66C- Identity theft.
 - Punishment- Imprisonment up to 3 years along with fine up to Rs.1 lakhs. [6]
- Section 66D- Cheating by personation by using computer resource.
 - Punishments- Imprisonment up to 3 years along with fine up to Rs.1 lakhs. [6]
- Section 66E- violation of privacy.
 - Punishment- Imprisonment up to 3 years or fine up to Rs.1 lakhs or both. [6]
- Section 66F- cyber terrorism.
 - Punishment- Life time imprisonment. [6]
- Section 67- publishing or transmitting obscene material in electronic form.
 - Punishment- Imprisonment up to 5 years along with fine which may extend up to Rs.1 lakhs (for first offence), Imprisonment up to 10 years along with fine which may extend up to Rs.2 lakhs (for second offence). [6]
- Section 67A- publishing or transmitting of material containing sexually explicit act, etc., in electronic form.
 - Punishment- Imprisonment up to 5 years along with fine up to Rs.10 lakhs (first offence), imprisonment up to 7 years along with fine up to Rs.20 lakhs (second offence). [6]
- Section 67B- publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.
 - Punishment- Imprisonment up to 5 years along with fine up to Rs.10 lakhs (first offence), imprisonment up to 7 years along with fine up to Rs.10 lakhs (second offence). [6]
- Section 73- publishing (electronic signature) Certificate false in certain particulars.

- Punishment- Imprisonment up to 2 years or fine up to Rs.1 lakhs or both. [6]
- Section 74- Publication for fraudulent purpose.
 - Punishment- Imprisonment up to 2 years or fine up to Rs.1 lakhs or both. [6]

2. The Information Technology (Amendment) Act, 2008-

2.1. Overview-

- The Information Technology (Amendment) Act, 2008 was enacted by the Parliament of India to amend the Information Technology Act, 2000. It received the President's assent on 5th February, 2009 and was officially published in the Gazette of India on the same day. [8]
- This act was introduced to address emerging cyber threats and challenges. This amendment has expanded the scope of cybercrimes offences such as cyber terrorism, identity theft, and data breaches. [9]

2.2. Objective-

- This act was introduced to strengthen the provisions of the IT Act, enhanced the penalties for cyber offences, and strengthen the cyber security measures in India. [9]
- The 2008 amendment act enhances several legal framework including cyber security provisions, data protection, identity theft, adjudication, and penalties. [10]

2.3. Key Provisions included under the 2008 amendment act-

- Section 66- Computer Related Offences.
 - Punishment- imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. [11]
- Section 66A- Punishment for sending offensive messages through communication service, etc.
 - Punishment- imprisonment for a term which may extend to three years and with fine. [11]
- Section 66B- Punishment for dishonestly receiving stolen computer resource or communication device

- Punishment- imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both. [11]
- Section 66C- Punishment for identity theft.
 - Punishment- imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh. [11]
- Section 66D- Punishment for cheating by personation by using computer resource
 - Punishment- imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. [11]
- Section 66E- Punishment for violation of privacy
 - Punishment- imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. [11]
- Section 66F- Punishment for cyber terrorism
 - Punishment- imprisonment which may extend to imprisonment for life. [11]
- Section 67- Punishment for publishing or transmitting obscene material in electronic form
 - Punishment- On first conviction, imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees.
 - On the second or subsequent conviction, imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees. [11]
- Section 67A- Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form.
 - Punishment- On first conviction, imprisonment up to five years and with fine up to ten lakh rupees.
 - On second or subsequent conviction, imprisonment up to seven years and also with fine which may extend to ten lakh rupees. [11]

3. Digital Personal Data Protection Act of 2023-

3.1.Overview-

- The Digital Personal Data Protection Act of 2023 was enacted by the Parliament of India. It received the President's assent on 11th August, 2023 and was officially published in the Gazette of India on the same day. [12]
- It is India's first comprehensive legislation governing individual's personal data. This act recognises both the rights of individuals to protect their personal data. [12]

3.2.Objective-

- To regulate how entities (Data Fiduciaries) collect, store, and process the personal data of individuals to ensure privacy.
- It grants certain rights to the individuals including, right to access information about their data, right to correction, and the right to erasure.
- It mandates that personal data can only be processed for a lawful purpose for which the individual has given consent, or for certain legitimate uses.
- It establishes obligations for data fiduciaries to maintain the security of data and report data breaches to the Data Protection Board of India. [13]

3.3.Key Provisions-

- Section 4- Grounds for processing personal data
- Section 6- Consent given shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action.
- Section 11- Right to access information about personal data.
- Section 12- Right to correction and erasure of personal data.
- Section 13- Right of grievance redressal.
- Section 14- Right to nominate.
- Section 16- Processing of personal data outside India.
- Section 26- Power of Chairperson
- Section 27- Power and Function of Board.
- Section 33- Penalties
- Section 37- Power of Central Government to issue directions.
- Section 40- Power to make rules. [12]

4. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

4.1.Overview-

- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were notified on 25th February, 2021, the Ministry Of Electronics and Information Technology under the Information Technology Act, 2000. [14]
- This act replaced earlier Information Technology (Intermediary Guidelines) Rules, 2011. The act provide regulations of electronic transactions and cybercrimes.

4.2.Objective-

- To bring internet based operations such as social media platforms, OTT streaming services, digital news outlets etc. within the ambit of the government regulation. [15]
- The act cast specific obligation on intermediaries to observe due diligence while discharging their duties. [16]
- The act also put obligation on the intermediary not to display, upload, modify, publish, transmit, upload or share any information that is obscene, pornographic, and invade the privacy of others. [16]

4.3.Key Provisions-

4.3.1. Part A- Intermediaries

- Obligations applicable to intermediaries
 - Annual notifications to users
 - Take down procedure
 - Grievance redressal mechanism
 - Retention of records
 - Assistance to the Government Agencies
 - Obligations for News and Current Affairs Content [17]
- Additional Obligations for Significant Social Media Intermediaries
 - Resident Officers and Local Presence
 - Identification of the first originator
 - Use of technology-based and automated tools
 - Monthly Compliance Report
 - Grievance redressal mechanism
 - Advertised or marketed services
 - Voluntary Verification for Users

- Notification of action taken against prohibited content [17]
 - Consequences of Non-Compliance with Part A
 - Intermediaries may lose their Safe Harbour Protection and be subject to the various liabilities as provided under the IT Act. [17]
- 4.3.2. Part B – Digital Media - Regulation of Publishers of News and Current Affairs and Online Curated Content
- New Definitions introduced
 - News and Current Affairs
 - Publisher of News and Current Affairs
 - Publisher of Online Curated Content
 - News Aggregator. [17]
 - Key Obligations
 - Code of Ethics
 - Requirement to Furnish Information
 - Adoption of a three-tiered regulatory framework for grievances
 - Disclosure Requirements on the Publisher
 - Retention of records. [17]

Landmark Cases-

1. State of Tamil Nadu v. Suhas Katti (2004) [18]

1.1.Overview-

- This case is popularly known as “The Suhas Katti Case”. This case is related to the posting of obscene, defamatory and annoying messages about a divorced woman in the yahoo message group.
- It has become one of the earliest cases under IT Act, 2000 where for the very first time the first ever conviction has been done. This case has set the bench mark in the Indian cyber history as it was solved by the Chennai Cyber Crime Cell within a short span of just 7 months after the filing of FIR.

1.2.Facts of the Case-

- In this case, the victim and accused were friends. Accused wanted to marry her but she refused him and marry another person. When she got divorced the accused again tried to approach her she again refused him. He started sending her late night messages and late night calls.
- Being aggrieved by the rejection, he started harassing and stalking her by posting her number on social media and started uploading obscene messages in the group. After this, the victim started receiving unwanted messages and phone calls from unknown number.
- The victim filed complaint in the Cyber Crime Cell. After filing of complaint, the police started tracing accused and finally arrested him. Charge sheet was filed against him under Section 67 of IT Act, 2000, Section 469 and 509 IPC before.

1.3.Judgment-

- The judgment was delivered by Ld. Additional Chief Metropolitan Magistrate on 5th November, 2004.
- The accused is found guilty of offences under section 469, 509 IPC and 67 of IT Act 2000.
- The accused is convicted and is sentenced for the offence to undergo rigorous imprisonment for 2 years under 469 IPC and to pay fine of Rs.500.
- For the offence under Section 509 IPC he is sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500.
- For the offence u/s 67 of IT Act 2000 to undergo rigorous imprisonment for 2 years and to pay fine of Rs.4000.

2. **Satyam Infoway Ltd v Sify net solutions Pvt. Ltd (2004)** [19]

2.1.Overview-

- This was the first case which deals with the Trademark and also the first case dealing with domain protection. In this case the Supreme Court pronounced that the Indian Trade Marks Act, 1999 is applicable for the regulation of domain name.
- The present case is related to the dispute regarding the domain name under the Intellectual Property Rights. This was a pivotal case decided on 4th May, 2004 by the Supreme Court of India.

2.2.Facts of the Case-

- In this case, the appellant, Satyam Infoway Ltd, incorporated in 1995 registered several domain names like www.sifynet, www.sifymall.com, www.sifyrealestate.com in June 1999 with the Internet Corporation for Assigned Names and Numbers (ICANN) and the World Intellectual Property Organisation (WIPO).
- The respondent, Sifynet solutions, started carrying on business of internet marketing under the registered domain names, www.siffynet.net and www.sijfynet.com which were similar to the appellant's domain names.
- When the appellant find that respondent is using their domain name for their business then the appellant filed a suit in the City Civil Court against the respondent. The court decided in favour of the appellant. Aggrieved by this decision, respondent filed an appeal before the High Court.

2.3.Legal Issues-

- Whether internet domain names are subject to the legal norms applicable to other intellectual properties such as trademarks?

2.4.Judgment-

- The Civil court observed that-
 - Appellant was the prior user of the trade name 'Sify' and they had earned good reputation in connection with the internet and computer services.
 - The court also held that the respondent's domain names were deceptive similar to the domain name of the appellant and it will cause confusion in the mind of the general public.
 - Therefore, the court ruled in favour of the appellant and grant temporary injunction against the respondent.
- The High Court observed that-
 - The respondent was doing business other than that done by the appellant and since there was no similarity between the two businesses, there was no question of customers being misled.
 - The court has ordered interim stay on the judgment of Civil Court.
- The Supreme Court held that-
 - The domain name fell under the ambit of Trade Mark Act and the court also held that allowing the respondent to further use the

domain name 'Siffy' would create confusion in the mind of the general public.

- The court granted an injunction in favour of the appellants. Decision of High Court is set aside. Appeal is allowed.

3. **Shreya Singhal v. Union of India (2015)** [20]

3.1.Overview-

- This case mark as one of the most important landmark supreme court judgment where 66A of the Information Technology Act, 2000 was struck down as it violate Article 19(1)(a) of the Indian Constitution, upheld Section 69A and read down Section 79.
- This case was decided on March 24, 2015 by the two-judge bench on the issue regarding online speech.

3.2.Facts of the Case-

- In this case, two girls were arrested by the Mumbai police for posting comments on Facebook for criticizing the bandh which was called by the memebers of Shiv Sena during the funeral of their leader Bal Thackery.
- Shreya Singhal who was the petitioner in this case filed a writ petition under Article 32 of the Constitution of India contending that Section 66A of the IT Act, 2000 violated Article 19(1) (a), which guarantees the right to freedom of speech and expression. The petitioner also challenged the constitutional validity of Sections 69A and 79 of the IT Act, 2000.

3.3.Legal Issues-

- Whether Section 66A of the IT Act violates the fundamental right to freedom of speech and expression under Section 19(1) (a) of the Indian Constitution?

3.4.Judgment-

- The court struck down Section 66A of the IT Act as it violates the fundamental right to freedom of speech and expression under Section 19(1) (a) of the Indian Constitution.
- The court also upheld Section 69A of the IT Act, 2000.
- The court also upheld the validity of Section 79 of the IT Act, and held that that intermediaries are required to take down content only after receiving a court order or notification from the appropriate government authority.

Emerging Issues in Cyber Law-

1. Data Privacy-

- In today's digital world, personal data has become extremely valuable. Digital platforms like e-commerce, online shopping sites, and e-banking are regularly collecting larger amount of person's personal data like address, mobile numbers, location, and biometric details. [21]

2. Data Breaches-

- In India, concerns regarding data misuse, and unauthorised sharing of personal information have increased significantly in recent years. Many people are still unaware of how their information is collected and used online. [21]

3. Artificial Intelligence-

- AI is increasingly used in healthcare, education, banking, finance, and law enforcement. AI-generated content is misused by the cyber attackers and causes political manipulation, financial fraud, defamation, and cyber harassment. [21]

4. Deepfake Technology-

- Now-a-days, this technology is increasing day-by-day. These technologies are creating fabricated pictures, audios, and videos by using artificial intelligence. From the above it is seen as real but in reality they are just fabricated. These are the growing tool for misinformation. [21]

5. Cyber Financial Frauds-

- The expansion of digital payment systems has increased the risk of UPI frauds, online banking scam, phishing attacks, and crypto currency-related crimes. There has been an increase in the financial losses across various states. [21]

6. Cyber Terrorism-

- Cyber-criminals are targeting government networks, financial institutions, healthcare system, and infrastructure posing a great risk to national security, and public order. [21]

7. Cross-Border Cyber Crime-

- Today, the crimes are not limited within the boundaries of one country. A single cyber offence may involve an offender, victim, server, and data

located in different countries. This creates serious legal difficulties, especially in deciding which country has the authority to investigate, prosecute, and punish the offender. [21]

Challenges Involved-

1. Rapid Technological Advancement-

- One of the biggest challenges in enforcing cyber law is the increase in technological development. Technology changes much more quickly than laws. As a result, legal provisions often become outdated before they can effectively deal with newly emerging technologies and cyber threats. [8]
- Cybercriminals are continuously adopting new techniques, lawmakers and enforcement agencies often find it difficult to keep up with the changing nature of cyber offenses. [22]

2. Lack of Specialised Expertise-

- Another major challenge in the enforcement of cyber law is the lack of technical expert. To deal with cyber security, digital forensics, electronic evidence collection, and data analysis we must need an expertise who has the advanced knowledge of how to deal with these problems. [22]
- Lack of expertise will affects the quality of investigation and also 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. [22]

3. Admissibility of Digital Evidence-

- Digital evidences such as emails, electronic records, online chats, IP addresses, CCTV footage, and computer data can be altered, deleted, copied, or manipulated easily without leaving any traces. [22]
- Since these evidences can be changed easily, maintaining the authenticity and reliability of such evidence has become very challenging. Cybercrime cases mainly depend on digital evidence. [22]

4. Low Reporting of cases-

- The major reason behind this is that there are many victims who still hesitate to approach the authorities because of embarrassment, social stigma and lengthy

proceedings. In some situations, many victim are unaware that they have become targets of cyber fraud. [22]

Suggestions for reforms-

1. The government should initiate widespread digital literacy programmes especially in rural and urban areas targeting vulnerable groups including children, women, and elderly.
2. Specialised cybercrime cells must be established in every state and district. They must be equipped with advanced tools.
3. For the quick and effective adjudication of cyber-related litigation, there is a need of specialised cyber law benches, dedicated cybercrime prosecutors, and judicial training programmes.
4. Digital courts and e-filing system must also be upgraded for handling the cyber-related litigation efficiently.
5. Police must be given training of how to handle digital evidences and international cooperation.
6. An Independent Data Protection Authority must be establish to prevent impartiality and investigate, audit, and penalises entries that violates privacy and data security norms. [23]

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. 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. [21]

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. [21]

Endnotes-

1. Axiom Law, Cyber Law Guide, <https://www.axiomlaw.com/guides/cyber-law> (last visited Aug. 2, 2026).
2. Pratik Yadav & Jully Garg, Emerging Information Technology and Cyber Laws: Issues and Challenges in India, *2 Motherhood Int'l J. Rsch. & Innovation* 89-92 (2025). <https://mhujournal.in/MIJRI/index.php/MIJRI/article/view/108/75> (last visited Aug. 2, 2026).
3. Kyle Chin, Top Cybersecurity Regulations in India in 2026, UPGUARD BLOG [Date of access: 2 August 2026, Time of access: 10:24 PM IST]. <https://www.upguard.com/blog/cybersecurity-regulations-india>.
4. Deepti Lata, Dr. RajVardhan, An Analytical Study of Cyber Law and Legal Framework in India, *INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN MULTIDISCIPLINARY PHYSICAL SCIENCES (IJIRMPs)* [Date of access: 2 August 2026, Time of access: 10:25 PM IST]. <https://www.ijirmps.org/papers/2025/2/232693.pdf>
5. Javed Iqbal & Bilal M. Beigh, Cybercrime in India: Trends and Challenges, *6 Int'l J. Innovations & Advancement Computer Sci.* 187 (2017).
6. Information Technology Act, No. 21, Acts of Parliament, 2000 (India), https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
7. Bhatt & Joshi Associates, Cyber Laws in India, <https://bhattandjoshiassociates.s3.ap-south-1.amazonaws.com/booklets+%26+publications/Cyber+Laws+in+India+-+Internet+Crimes%2C+Security+%26+Legal+Rights.pdf> (last visited Aug. 2, 2026).
8. Information Technology (Amendment) Act, No. 10, Acts of Parliament, 2009 (India), https://www.indiacode.nic.in/bitstream/123456789/15386/1/it_amendment_act2008.pdf
9. Kritika Kushwaha, Cyber Laws in India: Issues and Challenges, *5 Indian Journal of Legal Review (IJLR)* 361-371 (2025), <https://ijlr.iledu.in/wp-content/uploads/2025/04/V5I734.pdf>
10. Pallavi Ramesh Rao Gawande, Cybersecurity and Law in India: Issues and Challenges, *5 Int'l J. Advanced Rsch. Sci., Comm'n & Tech.* 129 (2025), <https://www.ijarsct.co.in/Paper23423.pdf>
11. Ministry of Home Affairs, National Cyber Crime Reporting Portal, Gov't of India, <https://cdn.s3waas.gov.in/s358d4d1e7b1e97b258c9ed0b37e02d087/uploads/2019/05/2019053179.pdf> (last visited Aug. 2, 2026).

12. Ministry of Electronics & Information Technology, Government of India, Report of the Expert Committee on the Digital Personal Data Protection Framework (2024), <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>
13. iValue Group, The DPDP Act: What You Need to Know (Feb. 6, 2024), <https://ivaluegroup.com/en-in/resources/blogs/the-dpdp-act-what-you-need-to-know/>
14. PRS Legislative Research, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, <https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021> (last visited Aug. 2, 2026).
15. Shardul Amarchand Mangaldas & Co., Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 Notified, <https://www.amsshardul.com/insight/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021-notified/> (last visited Aug. 2, 2026).
16. Telecom Review Asia, Government Strengthens Framework to Counter AI-Generated Deepfakes Through Legal Safeguards, Platform Accountability and Citizen Protection (July 31, 2026), <https://tele.net.in/national-news/government-strengthens-framework-to-counter-ai-generated-deepfakes-through-legal-safeguards-platform-accountability-and-citizen-protection-12214484>
17. Trilegal, Information Technology Rules, 2021 (Guidelines for Intermediaries and Digital Media Ethics Code) (Mar. 2, 2021), <https://trilegal.com/wp-content/uploads/2021/11/Information-Technology-Rules-2021.pdf>.
18. State of Tamil Nadu v. Suhas Katti, C.C. No. 4680 of 2004 (Ct. of the Chief Metro. Magistrate, Egmore, Nov. 5, 2004).
19. Satyam Infoway Ltd. v. Sifynet Solutions (P) Ltd., (2004) 6 S.C.C. 145.
20. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1.
21. Yashi Agarwal, Cyber Law in India: Emerging Issues and Challenges, 3 Int'l J. Rsch. L. & Mgmt. (Issue 9) (2026), <https://ijrlm.com/journal/cyber-law-in-india-emerging-issues-and-challenges/>.
22. Tanmaya Phani Aka, Jurisdictional Issues in Cross-Border Cybercrime, 2 Int'l J. Creative & Open Rsch. Eng'g & Mgmt. No. 3, at 1 (Mar. 2026),

https://www.researchgate.net/publication/401650717_Jurisdictional_Issues_in_Cross-Border_Cybercrime.

23. Pratyush Maurya, India's Cyber Laws in the Age of Rising Digital Threats: An Inquiry into Legal Efficiency and Reform, The Amikus Qriae, <https://theamikusqriae.com/research-paper-indias-cyber-laws-in-the-age-of-rising-digital-threats-an-inquiry-into-legal-efficiency-and-reform/> (last visited Aug. 2, 2026)