



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: Emerging Issues and Challenges

-Iffat Zehra

ABSTRACT:

This paper explores Indian cyber law's development since the passage of the Information Technology Act, 2000, and its current strains, arguing that lack of law is the prime hurdle. India has a new criminal law, a complete set of intermediary regulations, a data protection act, and a rising number of relevant constitutional verdicts. The prime problem is the amount and coherence of what's been built: too much relies on delegated legislation, there are few safeguards in cases that the State itself acts, and enforcement trails far behind the amount of online harm. Cybercrime and electronic evidence, intermediary liability and online speech, data protection, artificial intelligence and synthetic media, and surveillance and shutdowns are the five areas of stress analyzed in this paper that concludes with recommendations. As of October 2026, developments are reported.

Key Words: Cyber law, Information Technology Act, Intermediary liability, Data protection, DPDP Act, Deepfakes, Cybercrime, India

HYPOTHESIS:

Indian cyber law suffers from more the manner in which its regulations are crafted and enforced, than by an absence of legislation. Most of the remaining gaps are explainable through a heavy reliance on executive rule-making, insufficient protection against the State's own prerogatives, and enforcement which has not kept pace.

RESEARCH QUESTIONS:

1. To what extent is the system reliant on delegated legislation and how cohesive is it?
2. Are private entities and State parties bound by the guarantees equally?
3. What changes would be desirable and why are they inadequately enforced despite the adequacy of criminal law?

SCOPE OF RESEARCH:

The paper is limited to Indian law and to the period up to October 2026. It focuses on the law relating to cyberspace, which comprises three levels – primarily statutes (Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023, Digital Personal Data Protection Act, 2023, Telecommunications Act, 2023, Promotion and Regulation of Online Gaming Act, 2025), subordinate and executive laws (Intermediary Rules of 2021 as amended in 2026, the 2009 blocking and interception rules, DPDP Rules of 2025 and CERT-In directions of 2022), and case law (Supreme Court and High Court decisions). Within this broad area, the paper addresses, in the context of the case law, five issues: cybercrime and electronic evidence; intermediary liability and freedom of speech; data privacy; artificial intelligence and deepfake; surveillance and internet shutdowns. Jurisdiction and international aspects are briefly discussed. Intellectual property, e-commerce and consumer protection, digital taxation, competition law, or sector specific regulations of the RBI and SEBI are outside the scope of this paper, except to the extent they are directly relevant to the topics identified above. The paper uses foreign and India-specific materials for comparison and background only. Finally, pending cases are identified as such, and no attempt is made to forecast likely outcomes.

RESEARCH METHODOLOGY:

The nature of research undertaken is doctrinal and analytical. The study is based upon close examination of authoritative legal texts with no reference to fieldwork, as the hypothesis requires an assessment of the very structure of the legal framework: what sources of authority it comprises and which bodies are bound by it. Primary sources include statutes, rules, notifications, executive directions and published judgments of the Supreme Court and the High Courts. Secondary sources include books, law-review articles, official reports, and legal and news commentary, which are drawn upon primarily for very recent developments. Where a point relies upon a secondary or press account, this is indicated in the citation. Statistics, such

as those provided by the National Crime Records Bureau, are used to illustrate the scale of the problem and should not be taken as precise measurements. The analysis undertakes mapping of the statutory architecture; examines each of the five areas against the leading cases and scholarship; compares the safeguards on private actors with those on the State; and then extracts recommendations. Given that the study is based upon no interviews or case-file examination, its conclusions on enforcement rely on published data, which are themselves often incomplete. Citations follow the Bluebook 20th edition, adapted for Indian authorities.

INTRODUCTION:

When Parliament passed the Information Technology Act in 2000, it was largely concerned about contracts. The first purpose of the act, which was based on the United Nations Model Law on Electronic Commerce, was to state that digital signatures could replace ink and that electronic records might be just as good as paper ones (Anon., 2000). Cybercrime was practically an afterthought, included as a brief chapter of offenses to make the Act appear effective. The main event has become the major event, the main event. In India, the majority of persons who encounter cyber law do so as victims of fraud, users of platforms that have just deleted posts, or people whose phone number has appeared in the database of a stranger.

This paper aims to discuss the Indian law development as of October 2026. The problem is complicated by the fact that the current situation is characterized by a number of complaints about the inadequacy of India's cyber laws. There is a sufficient formula that ceased to be relevant. Now, India has a law on synthetic media, a new criminal code, extensive intermediary regulations, a data protection act, and a growing number of constitutional court decisions shaping digital rights. But how do all these elements fit together? Is there a common concept behind them?

Here, we argue that most of the current issue can be related to the three structural characteristics. The first is a significant reliance on the executive instruments and delegated law, which means that the rules on platform obligations, speech, and privacy are usually drawn up by ministries, not debated in the Parliament. The second is an uneven distribution of safeguards: obligations for private companies have been increasingly detailed in time, while State's own power to block, intercept, collect, and exempt have remained thin. The third is a disconnect between the law and its implementation, which is best illustrated by the amount of online financial fraud that law enforcement and courts are having difficulty handling. These

are not unique to India. However, as a whole, they do affect how Indian cyber legislation is currently failing and thriving.

The following is a list of the order in which the discussion proceeds. Statutory frameworks are presented in Part II. Data privacy, artificial intelligence and deepfakes, cybercrime and digital evidence, intermediary liability and freedom of expression, surveillance, and internet shutdowns are each taken up in Parts III through VII, respectively. International aspects and jurisdictional issues are discussed briefly in Part VIII. Part IX contains concluding remarks. A doctrinal methodology has been applied, relying on case law, statutes, regulations, and scholarly commentary on these topics.

I. THE STATUTORY ARCHITECTURE:

The majority of today's cybercrime and surveillance tools are based on a major change to the IT Act of 2000 in 2008 (Anon., n.d.). It provided the legal basis for CERT-In under section 70B, created offenses such as identity theft (section 66C), cheating by personation using a computer resource (section 66D), violation of privacy (section 66E) and cyberterrorism (section 66F), gave the government extensive interception and blocking powers under sections 69 and 69A, and updated the liability of intermediaries under section 79. Of note, the infamous Section 66A, which made sending "offensive" messages illegal, was also part of this amendment and was subsequently repealed by the Supreme Court.

The rules around sensitive personal data from 2011, created under section 43A of the Act, provide the reasonable security guarantees framework (Anon., 2011). Two sets of regulations concerning blocking and interception were issued in October 2009 (Anon., 2009). The Intermediary Guidelines and Digital Media Ethics Code of 2021, which have since been amended several times, concern themselves with obligations of platforms. CERT-In, the computer emergency response team, issued legally binding directions for incident response and record retention in 2022 (Anon., april 2022). A diligent reader seeking to understand the law's effect on a medium that hosts online services would have to consult a statute, four sets of rules, a ministerial direction, and a few court rulings, and then determine which of them had been amended since.

The image has been captured since 2023. The offenses of cheating, personation, stalking, voyeurism, defamation, and so forth have been brought under the purview of the Bharatiya Nyaya Sanhita, which replaced the Indian Penal Code in July 2024 (Anon., 2023). It has also incorporated a chapter on organized-crime to deal specifically with cyber offenses. The

directions for proving electronic documents were revised by the Bharatiya Sakshya Adhiniyam (Anon., 2023). The Telegraph Act has been superseded by the Telecommunications Act, 2023, which regulates suspension of services and other matters (Anon., 2023). The country now has a general privacy law in the shape of the Digital Personal Data Protection Act, 2023 (Anon., 2023). A bill to prohibit the purchase of internet games was passed by the Parliament in August 2025 (Anon., 2025).

The anticipated consequence is overlap. The IT I T sector may be booked under the same legislations as BNS. In *Sharat Babu Digumarti*, the Supreme Court tried to enforce a judicial order which determined that the general criminal law will be overruled by a specific one if the IT Act covers a particular issue, such as the obscenity of electronic information (*Sharat Babu Digumarti v. Gov't (N.C.T. of Delhi)*, 2017). This reasoning is convenient and beneficial in specific cases; however, it does not refer to which law the investigator and prosecutor should follow first. Defense lawyers often use this dilemma to benefit their clients in cybercrime cases. Institutional problems have also been interfering with judicial activities regarding the IT Act: in 2017, the Cyber Appellate Tribunal was merged with the Telecom Disputes Settlement and Appellate Tribunal, which was already at maximum capacity (Anon., 2017).

II. CYBERCRIME, ENFORCEMENT AND ELECTRONIC EVIDENCE:

a. THE SCALE OF THE PROBLEM:

While the interpretation of these figures is open to debate, the figures themselves are not. Around 86,000 cybercrime incidents were reported by the National Crime Records Bureau in 2023, up 31 percent from 65,893 in 2022 (Anon., 2025). Most of them, however, are the result of fraud schemes. Yet only encompasses those that advanced to the stage of a First Information Report, and that is where the true attrition begins. There were approximately 22.68 lakh complaints on the national website in 2024, with claimed losses of over ₹22,846 crores, according to data ascribed to the Indian Cyber Crime Coordination Centre. Only 1.9 percent of portal complaints in 2023 were converted into formal complaints (Anon., 2025). The pattern is obvious regardless of the precise numbers. Only a small percentage of the injury is captured by the law, and even less of it is addressed.

b. THE “DIGITAL ARREST” EPISODE:

The most recent example was the rise in digital arrest scams in which conmen contacted the victims through video conferences and held them on the line for hours or even days in some cases while saying that they were under investigation by the CBI or the Enforcement Directorate and them to pay money into a “safe” account. In October 2025, the Supreme Court took suo moto cognizance of the alleged swindle after an elderly couple from Ambala fell prey to the conmen after being shown fake orders of the Supreme Court and losing over a crore of rupees (Anon., n.d.). On December 1, 2025, the Court ordered an inquiry by the states and directed the CBI to probe these matters initially and look into the role of the bank officials whose accounts had been used. By August 2026, it had issued detailed directions to the Reserve Bank, the Centre, the states, and the telecom department. One of the directions pertained to developing a standard operating procedure concerning mule accounts (Anon., n.d.).

There are two lessons to be learned from this. The first is that the problem was never the substantive offenses, as the BNS and the IT Act already penalize extortion, personation, and cheating. The infrastructure around them was inadequate: police did not have resources and jurisdiction to trace money across state lines, banks opened accounts with unreasonable ease, telecom companies sold connections in bulk with little scrutiny, and the reporting mechanism was flawed, leaving victims stranded in the critical first hours when the money could have been traced. The second lesson, however, is more disconcerting. It is not legislation or the administration but a court that has taken up the responsibility of regulating the sector, at least for now. A set of procedural orders from the court would be insufficient in the long run. There needs to be a comprehensive legal framework that makes banks and telecom companies accountable and lays down punishment norms in case of negligence.

c. ELECTRONIC EVIDENCE:

The case still needs to be proved even when the offender has been identified. Indian jurisprudence has been highly inconsistent when it comes to this exact issue. According to the ruling made in *Anvar P.V. v. P.K. Basheer*, the recordings made electronically could only be proved as secondary evidence along with the certificate issued under the section 65B of the Evidence Act (*Anvar P.V. v. P.K. Basheer*, 2014). In cases where the petitioner fails to obtain the required certificate, the later bench ruled that such certificate would no longer be required. (*Shafhi Mohammad v. State of H.P.*, 2018) However, a bigger bench of the Supreme Court overturned this decision in *Arjun Panditrao Khotkar* case, restoring the original ruling. However, it was acknowledged that the certificate could be compulsory in particular

circumstances (Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020). Section 63 of the new Bharatiya Sakshya Adhiniyam, which replaces the previous section 65B, requires that the certificate be signed not only by an expert but also by the person who has operative control of the computer or other device mentioned in the affidavit (Anon., 2023).

The practical effect is that a bank statement, a chat log or a CCTV recording can be excluded for want of a properly drafted certificate, even if no one doubts its authenticity. Digital evidence is fragile and easily manipulated, says Orin Kerr, in a separate legal system, as he puts it, and procedure must take that into account (Anon., n.d.). But neither accuracy nor fairness are protected by a formal rather than substantive certificate requirement. A system that sees the certificate as the principal protection and gives judges no feasible mechanism to evaluate the integrity of the underlying data via hash values, chain-of-custody records and forensic analysis gets the priorities slightly wrong. The issue will probably get worse before it improves if the expert signature requirement is implemented without prior strengthening of forensic capabilities in the police at district level and in the courts.

III. INTERMEDIARY LIABILITY AND ONLINE SPEECH:

The provision of Section 79, which gives conditional immunity to intermediaries for any third-party content, forms the basis of India's platform regulation. The foundational decision constraining online free speech in India is the Shreya Singhal case of 2015 (Shreya Singhal v. Union of India, 2015). By striking down Section 66A as being overly broad and limiting and not falling under permissible restrictions of free speech under Article 19(2) the Supreme Court ruled that Section 69A and the blocking rules (which require a presidential order for blocking content) are sufficiently precise and do not violate the constitution (Anon., n.d.). The blocking orders were also clarified to require the presence of a committee, a hearing, and a written justification. In addition, the Court modified Section 79(3)(b) to interpret it as requiring removal only in response to a court order or government notification concerning any of the grounds specified in Article 19(2). Gautam Bhatia notes that the Singhal ruling was the Supreme Court's most significant free-speech judgment, and this appears to be an appropriate assessment. The judiciary has also demonstrated its awareness of the Safe Harbour rules, as demonstrated by the Delhi High Court's division bench ruling in MySpace that required notice-and-takedown procedures based on Section 79 read with the Copyright Act and not continuous monitoring (MySpace Inc. v. Super Cassettes Indus. Ltd., 236 (2017) D.L.T. 478 (Del.) (India); Google India Pvt. Ltd. v. Visakha Indus., (2020) 4 S.C.C. 162 (India), n.d.). The Supreme

Court has also stated on several occasions (most recently in the Visakha Industries case) that intermediaries should not be held to a standard of constant vigilance.

A decade later, the story of partial victory and persistent slippage takes center stage. The most stunning example of this is perhaps the infamous section 66A itself. Though struck down in 2015, it continued to be enforced in police stations for years. As a result, the Supreme Court pulled out the plug on all ongoing cases and forbade new ones in 2022 (*People's Union for Civil Liberties v. Union of India*, W.P. (Crim.) No. 199 of 2013 (India July 5, 2022), n.d.). A section was thus another case of a loophole practically still in force. It is a minor flaw in India's digital regulation, though, compared to the fact that when the law changes, the people responsible for implementing it are not notified of it.

Another form of amendment is represented by the Intermediary Rules of 2021. They require that social media giants' intermediaries appoint resident compliance officers, handle grievances, remove particular posts within certain time limits, and, in the case of messaging services, make it possible to identify the "first originator" of a message. While all of these requirements are debatable, the traceability requirement under Rule 4(2) received the most criticism. WhatsApp is currently challenging this requirement before the Delhi High Court in May 2021, arguing that it cannot be achieved without undermining end-to-end encryption, that it fails the proportionality test put forward by Puttaswamy and that it violated the scope of rules under section 79. As far as published documents indicate, the challenge, together with a series of petitions transferred to the Delhi High Court by the Supreme Court in 2024, is pending. The dispute serves as an excellent example of Lawrence Lessig's thesis that a system's architecture governs behaviour just as surely as a statute: requesting a messaging service to trace originators is tantamount to requesting to change its offerings.

The courts' willingness to defer to the executive has not been universal, however. In September 2024, the Bombay High Court in Kunal Kumar Kamra's case ruled against a 2023 amendment to the Intermediary Rules by the ministry. The amendment would have allowed government-owned fact checkers to identify government-related content as fake or false, removing protection for intermediaries who hosted it. A year later, X Corp.'s petition challenging the Sahyog portal, which relays takedown notices from federal and state authorities to social media platforms, was rejected by the Karnataka High Court. The Court is a source of the court, which is itself, which is itself, which is itself, which is itself, which is itself, which is itself.

The verdict's significance stems from what it says about the system Shreya Singhal was part of. Based on a more accurate reading of that judgment, the State's ability to force the takedown was found in section 69A, along with its hearing, reasons, and review. Losing a platform's immunity was covered in Section 79. There are now two channels: one with procedural protections and another with far fewer if section 79(3)(b) can also allow directives from a range of officials through a portal. Although it is beneficial, an October 2025 revision limiting the officers who might issue such notices to the higher grades does not change the underlying philosophy. Governments may favor the faster route, platforms may acquiesce to preserve their immunity, and the impacted user--who is often unaware of this--may have nowhere to turn. Big platforms are the new governors of Internet expression, according to Kate Klonick. India's approach has evolved from allowing such governors to control them with minimal oversight and using the threat of losing immunity as a lever.

IV. DATA PROTECTION AND THE DPDP ACT:

India did not have a general privacy law before a few years. In Justice K.S. Puttaswamy (Retd.) v. Union of India nine judges laid down the constitutional basis for privacy in 2017, ruling that it is a fundamental right inherent in article 21 and setting out a three-step test for any infringement on it: legality of the processing, legitimate aim and proportionality. In 2018 the court upholds Aadhaar with significant limitations upon applying this test to it. The Srikrishna Committee drafted a law in 2018 and after a long and torturous legislative process the DPDP Act came into force in August this year.

The Act is founded upon the notions of a data principle, that is to say, the individual to which the data pertains, and a data fiduciary, which determines the purpose and manner in which personal data is processed. Consent or one of the enumerated "legitimate uses" is required for processing, fiduciaries must implement reasonable security precautions and report breaches, individuals have a right of access, correction, erasure and grievance redress, and processing of children's data for those under the age of eighteen requires verifiable parental consent and prohibits tracking and targeted advertising, failure of which can lead to penalties of up to ₹250 crore enforced by a Data Protection Board. The mechanism of implementation is provided within the Digital Personal Data Protection Rules, 2025, which were announced on November 14, 2025. The obligations are implemented incrementally, where most of the substantive duties come into effect approximately eighteen months later, in May 2027.

While the Act's virtues are manifold, its weaknesses are substantial, and several of them strike at the heart of the Puttaswamy promise. Most evidently, it is the treatment of the State. The way in which it is handled, the most evident of all, is covered in section 17. The central government may notify any State instrumentality of its exclusion from the operation of the Act on grounds of security, sovereignty, and public order by notification. The exemption does not have to be necessary, reasonable, or subject to independent scrutiny. It is hard to reconcile a right that the Court has declared that binds the state first with a regulation that regulates the private sector closely, leaving the nation's largest data collectors up to the whim of the executive.

The effect on transparency is the second concern. The Right that the public information is the public information is the public information. The officials may decide to withhold information concerning public employees, those who have received assistance from government agencies, and other matters on the grounds of privacy because of the broad interpretation of personal information. Privacy and transparency are meant to balance each other, but the amendment tips the scales in favor of the former, not necessarily by design but by statute.

Thirdly, the Act removes the right to compensate, the right to compensate, the right to compensate, the right to compensate. The DPDP Act proposes penalties paid to the State and not to the individual whose data was exposed and Section 43A of the IT Act which allowed individuals to claim damages for a failure to protect sensitive data has been revoked. Therefore, a person whose financial information is compromised may have the right to file a complaint to the Board but will not be entitled to any legal compensation. Fourthly, the independence of the Board is questionable due to the fact that its terms of service and composition are decided by the central government which is also the biggest fiduciary it will be asked to regulate.

Additionally, there are conceptual difficulties beyond the reach of India-specific solutions. Even if users would not read the alerts, and even if they could understand them when they read them, consent is necessarily a solution; Daniel Solove's scorn for "privacy self-management" is particularly relevant in the context of both heavy mobile phone use and low digital literacy in India. Fiduciaries will be obliged to adopt the verifiable parental permission (VPP) model for under-eighteens to determine a parent from a minor, which is a euphemism for collecting more data. Anupam Chander and Uyên Lê have documented the wiser "data nationalism" that emerges when sector regulators enforce local storage of information as a default while allowing

third-party processing anywhere else, unless the jurisdictions involved are on an exclusionary list maintained by central governments. Most importantly, it was not explained how the two regimes for breaching data secrecy differ and coordinate: responding to the 2022 directions requires notification to CERT-In within six hours, whereas the DPDP Act requires notification to the Board and the affected persons.

V. ARTIFICIAL INTELLIGENCE, SYNTHETIC MEDIA AND NEW TECHNOLOGIES:

The deepfake problem was quick to invade the Indian public consciousness before legislation could catch up to it. Robert Chesney and Danielle Citron's worst fears have already materialized. Fake, realistic video and audio can be used for scams, political manipulation, and worst of all, non-consensual pornography. For a while, the government relied on notices to platforms and old laws like the IT Act and the BNS. After the draft was shared in October, it announced an updated to the Intermediary Rules in February 2026 that for the first time defined "synthetically generated information".

According to the amendment, 'audio, visual, or audio-visual content that is artificially or algorithmically created or altered so that it appears real' is defined. It directs that such content should be clearly identified and contain unalterable provenance metadata. It further requires major social media intermediaries to acquire and verify user statements, drastically reducing takedown durations to two hours for non-consensual intimate imagery and three hours for lawful orders, and shortening the time frame for grievance redress from fifteen days to seven. The objective is explicit, and a clear labelling guideline is preferable to silence.

The specifics are where the issues are. A fraudulent text created by a language model or an AI-generated text that spreads misinformation would not be covered by the proposed definition since it only mentions audio and visual content. Statements made by users must be evaluated using detection technologies, which is problematic because platforms are likely to significantly label content, not label it, or merely accept it at face value. Safe harbour depends on compliance, so it makes sense for firms to remove orders if the three-hour deadline is insufficient for moderators to assess whether a given order is unlawful, much less justify it. This problem of excessive removal is well-known in other areas of law; by exacerbating the issues in Part IV, the amendment makes them even more difficult to resolve. The amendment covers "intermediaries" more generally than just platforms in the new rules. As a result, it does not address generative systems' developers, trainers, and automated procedures, and the

responsibilities that should be placed on them, or the liabilities that arise when things go wrong. India has no comprehensive artificial intelligence law, and the same structural deficit will persist if the rules are changed in the wrong way.

The ban on online gaming reflects the same pattern of conduct in another sphere. The 2025 Act absolutely bans real-money online games, whether purely skill-based or chance-based, in contravention of a body of case law that had gradually developed around this distinction. The objections to it, which the Supreme Court transferred to itself in September 2025, range from questions of proportionality to challenges to Article 19(1)(g) and to the constitutional separation of legislative functions between the Union and the states. Regardless of the outcome, the choice between an absolute prohibition and the imposition of licensing, expenditure caps and age limits suggests that in the face of rapidly advancing technologies and real dangers to others, this approach will prevail.

VI. SURVEILLANCE AND NETWORK SHUTDOWN:

In India, the state controls the communication on the basis of few laws and lots of customs. In India, with directions issued by Home Secretary and evaluated by a committee that only consists of the executive authorities, the government may order interception, surveillance, and decryption in the name of sovereignty, security, and law and order, according to Section 69 of the IT Act and Interception Rules. In PUCL, the Supreme Court had laid down rules concerning the tapping of telephones in 1997. However, they are incorporated in the executive regulations, which are not subjected to the appraisal of an autonomous supervising agency. Not much has improved since the evaluation of these safeguards by Chinmayi Arun, published over ten years ago, showed their paper-thin nature. The Pegasus episode had demonstrated the point with concrete examples. The government had not cooperated as expected when the Supreme Court, in the installation of a technical committee in 2021, inquired into the allegations of the use of spyware.

A related topic is the issue of net shutdowns. The Court in *Anuradha Bhasin* has held that such orders must be disclosed, proportional and subject to judicial review, and that it is unlawful to suspend internet services indefinitely. Nonetheless, such shutdowns have continued. In 2024 alone, according to Access Now, there were 84 in India, amongst the highest rate in the world. The power to suspend services is now regulated by the Telecommunications Act, 2023 and regulations promulgated thereunder in 2024, which have replaced the earlier legal order. But the problem that orders are issued on dubious grounds, seldom disclosed and subject to a

hurried review process, remains. As Smriti Parsheera's work has demonstrated, such is the pattern of use of facial recognition by the police, which operates without a legal framework, a similarly troubling pattern of expanded powers and minimal oversight.

VII. JURISDICTION AND INTERNATIONAL COOPERATION:

The IT Act's Section 75 applies to acts by persons located outside of India if the offense involves an Indian computer or network. There are no reasonable methods of implementing the broad implications of this provision. The procedure of mutual legal aid in India is slow enough that money is usually gone before a request can be granted, and evidence in a fraud investigation will often be stored by a company in the United States or Ireland. The claim by Jack Goldsmith and Tim Wu that governments may in fact enforce the internet by pressuring local intermediaries may be seen in practice in India, where platforms have been required to hire local officers and store data domestically in order to deal with the problem of foreign data. Cross-border evidence is not produced by that method, but compliance is.

Due to its controversial provisions on cross-border data access and sovereignty, India has not ratified the Council of Europe treaty on cybercrime. A separate convention against cybercrime, negotiated in a more open environment, was adopted by the UN General Assembly in December 2024. The issue of India's accession to the deal and any accompanying reservations or human rights protections should be subject to open debate in parliament rather than being decided administratively.

VIII. RECOMMENDATIONS:

The recommendations above lead to the following conclusion. Rather of being all-encompassing, they are meant to be helpful.

Firstly, the legislation should take the place of subordinate rules as the foundation of platform regulation. The duties of intermediaries, the conditions of safe harbor, and the grounds and procedures for takedown should be established by Parliament after discussion, regardless of whether it looks like the much-talked-of Digital India Act instead of amending the IT Act. It will stop courts from having to hear multiple times if a ministry was authorized to formulate a particular rule.

Secondly, India needs to streamline its takedown and blocking processes through one procedure including protections which *Shreya Singhal v. Union of India* found essential, namely, rational written orders, notice to the originator wherever feasible, a right to be heard,

independent review and regular disclosure of aggregated statistics. There must be a clear appeal process for users who have had content removed, and limits on the time for compliance should give users a fair opportunity to ascertain legality.

Thirdly, exemptions to the DPDP Act's section 17 need to be subject to time limitations, oversight by an impartial agency and a statutory test of necessity and proportionality to reinstate a public interest override. The modification to the Right to Information Act should be reviewed to provide a legal remedy to data principals.

Fourthly, instead of a mere administrative step, enforcement capacity should be seen also as a legal requirement. This would include mandatory obligations for banks and telecom companies to verify accounts and SIMs, fixed deadlines for freezing suspected proceeds of fraud, budget allocation at the level of districts for forensic laboratories, the obligation to register a formal complaint if a complaint uncovers a prosecutable crime, and a statutory plan for returning the victims' money. This is suggested by the Supreme Court's mandates regarding digital arrests, but ought to be put on a statutory basis.

Fifthly, the integrity of the data should take precedence over the certificate in the regulations pertaining to electronic evidence. The requirement of an expert signature mandated in section 63 Adhiniyam should only be implemented if there is available forensic capacity to back it and courts should be authorized and trained to rely on hash verification and forensic reports.

Sixthly, any regulation of synthetic media should be based on a risk basis, apply to both text and generative system developers, and combine short takedown windows with substantive procedural safeguards for platforms and users. It would be preferable to adopt a general artificial intelligence law, following consultation, rather than amending it in piecemeal fashion.

Seventhly, India should take the United Nations Convention against Cybercrime seriously, and update its mutual legal assistance policy, ensuring that any opt-in includes specific human rights protections.

IX. CONCLUSION:

It is tempting to chart India's jurisprudence on cyber law over the last 25 years as a steady, if sometimes surprising, advance of regulation. It is also tempting to view it as a series of responses to fundamentally easy questions about who regulates whom, who gets to know what, and what recourse is available to the harassed and defrauded individual in the digital age. Courts in *Shreya Singhal*, *Puttaswamy*, and *Anuradha Bhasin* have had no issue in upholding

constitutional values, if sometimes with the hesitation of delegated legislation. At the same time, as the Sahyog judgment and the DPDP exemptions show, they have also been willing to allow the executive to go where the Constitution would not. Therefore, while the push to introduce fresh legislation to govern newer technologies is appropriate, it is not the only task before lawmakers in the near future.

It is, perhaps, more important to begin thinking about ends than means. If netizen sovereignty is to be achieved, symmetric protection is necessary for both the State and the private actor; if rights are to be meaningfully enforced, the instruments of their enforcement need to be created with the same care as the rights themselves; and if the big questions are to be genuinely answered, they must be framed in Parliament and not in the mystique of notification. India has passed laws that allow such a cyber-settlement to emerge, and therefore has the wherewithal to complete it. It is less clear that it has the will to do so.

X. REFERENCES:

Cases

1. Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
2. Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).
3. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).
4. Google India Pvt. Ltd. v. Visakha Indus., (2020) 4 S.C.C. 162 (India).
5. In re Victims of Digital Arrest Related to Forged Documents (India Oct. 17, 2025) (order taking suo moto cognizance).
6. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
7. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 S.C.C. 1 (India).
8. Kunal Kamra v. Union of India, Writ Pet. (L) No. 9792 of 2023 (Bom. Sept. 20, 2024) (India).
9. Manohar Lal Sharma v. Union of India, 2021 SCC Online SC 985 (India).
10. MySpace Inc. v. Super Cassettes Indus. Ltd., 236 (2017) D.L.T. 478 (Del.) (India).
11. 1People's Union for Civil Liberties v. Union of India, (1997) 1 S.C.C. 301 (India).
12. People's Union for Civil Liberties v. Union of India, W.P. (Crim.) No. 199 of 2013 (India July 5, 2022).
13. Shafhi Mohammad v. State of H.P., (2018) 2 S.C.C. 801 (India).
14. Sharat Babu Digumarti v. Gov't (N.C.T. of Delhi), (2017) 2 S.C.C. 18 (India).
15. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

16. WhatsApp LLC v. Union of India (Del. filed May 2021) (India).
17. X Corp. v. Union of India, W.P. No. 7405 of 2025 (Kar. Sept. 24, 2025) (India).

Constitutional Provisions, Statutes and Subordinate Legislation

18. India Const. arts. 19, 21.
19. Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
20. Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).
21. Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
22. Digital Personal Data Protection Rules, 2025 (India) (notified Nov. 14, 2025).
23. Finance Act, 2017, No. 7, Acts of Parliament, 2017 (India).
24. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
25. Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).
26. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (India) (notified Feb. 10, 2026; in force Feb. 20, 2026).
27. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India).
28. Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, G.S.R. 781(E) (Oct. 27, 2009) (India).
29. Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, G.S.R. 780(E) (Oct. 27, 2009) (India).
30. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (Apr. 11, 2011) (India).
31. Promotion and Regulation of Online Gaming Act, 2025, Acts of Parliament, 2025 (India).
32. Right to Information Act, 2005, No. 22, Acts of Parliament, 2005 (India).
33. Telecommunications Act, 2023, No. 44, Acts of Parliament, 2023 (India).
34. Telecommunications (Procedures and Safeguards for Temporary Suspension of Services) Rules, 2024 (India).
35. Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, No. 20(3)/2022-CERT-In (Apr. 28, 2022) (India).

Books

36. GAUTAM BHATIA, OFFEND, SHOCK, OR DISTURB: FREE SPEECH UNDER THE INDIAN CONSTITUTION (2016).
37. JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).
38. LAWRENCE LESSIG, CODE: VERSION 2.0 (2006).

Articles

39. Chinmayi Arun, Paper-Thin Safeguards and Mass Surveillance in India, 26 NAT'L L. SCH. INDIA REV. 105 (2014).
40. Anupam Chander & Uyên P. Lê, Data Nationalism, 64 EMORY L.J. 677 (2015).
41. Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 CALIF. L. REV. 1753 (2019).
42. Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 COLUM. L. REV. 279 (2005).
43. Kate Klonick, The New Governors: The People, Rules, and Processes Governing Online Speech, 131 HARV. L. REV. 1598 (2018).
44. Smriti Parsheera, Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?, Data Governance Network Working Paper No. 5 (2019).
45. Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880 (2013).

Reports, International Instruments and Government Documents

46. Access Now, EMBOLDENED OFFENDERS, ENDANGERED COMMUNITIES: INTERNET SHUTDOWNS IN 2024 (2025).
47. Comm. of Experts Under the Chairmanship of Justice B.N. Srikrishna, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS (2018).
48. Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.
49. G.A. Res. 51/162, U.N. Doc. A/RES/51/162 (Dec. 16, 1996).
50. G.A. Res. 79/243 (Dec. 24, 2024).
51. Group of Experts on Privacy, REPORT OF THE GROUP OF EXPERTS ON PRIVACY (Planning Comm'n 2012).
52. Nat'l Crime Recs. Bureau, Ministry of Home Affairs, CRIME IN INDIA 2023 (2025).

News Reports, Commentary and Online Sources

53. AZB & Partners, India's Digital Personal Data Protection Act: Phased Rollout and Key Compliance Milestones (Nov. 14, 2025), <https://www.azbpartners.com/?p=87799>.
54. Challenge to the Promotion and Regulation of Online Gaming Act, 2025, SUPREME COURT OBSERVER, <https://www.scobserver.in/cases/challenge-to-the-promotion-and-regulation-of-online-gaming-act-2025/> (last visited Oct. 4, 2026).
55. Debayan Roy, Supreme Court Orders CBI Probe into Digital Arrest Scams, BAR & BENCH (Dec. 1, 2025), <https://www.barandbench.com/news/supreme-court-orders-cbi-probe-into-digital-arrest-scams>.
56. Editorial, NCRB Needs to Be More Up to Date, DT NEXT (2025), <https://www.dtnext.in/amp/story/edit/editorial-ncrb-needs-to-be-more-up-to-date-848407>.
57. Hogan Lovells, India Introduces Mandatory Labelling for AI and 3-Hour Takedown for Illegal Content (2026), <https://www.hoganlovells.com/en/publications/india-introduces-mandatory-labelling-for-ai-and-3hour-takedown-for-illegal-content>.
58. IT Rules 2026, IPLEADERS BLOG, <https://blog.ipleaders.in/it-rules-2026/> (last visited Oct. 4, 2026).
59. Moneylife Digital Team, Supreme Court Issues Directions to Curb Digital Arrest Scams, Asks RBI to Frame SOP on Mule Accounts, MONEYLIFE (Aug. 4, 2026), <https://www.moneylife.in/article/supreme-court-issues-directions-to-curb-digital-arrest-scams-asks-rbi-to-frame-sop-on-mule-accounts/81256.html>.
60. Press Trust of India, Delhi HC Adjourns Hearing on Facebook, WhatsApp Pleas Challenging IT Rules on Traceability to August, UDAYAVANI (Apr. 25, 2024), <https://udayavani.com/?p=1634573>.
61. Press Trust of India, NCRB Data Shows Rise in Cybercrimes Using Mobile Phones and Computers, All India Radio (Dec. 5, 2025), <https://www.newsonair.gov.in/ncrb-data-shows-rise-in-cybercrimes-using-mobile-phones-and-computers/>.
62. Press Trust of India, Supreme Court Takes Suo Motu Cognisance of Digital Arrest Scams, Seeks Response from Centre, CBI, MONEYLIFE (Oct. 2025), <https://moneylife.in/article/supreme-court-takes-suo-motu-cognisance-of-digital-arrest-scams-seeks-response-from-centre-cbi/78615.html>.

63. Resemble AI, India IT Rules Amendment 2025 (Deepfake Provisions), <https://www.resemble.ai/laws-and-regulations/india-it-rules-amendment-2025-deepfake-provisions> (last visited Oct. 4, 2026).
64. Shailesh Kumar, Del HC | WhatsApp Challenges Intermediary Rules, Says Traceability Will Break End-to-End Encryption, Breach Privacy, SCC ONLINE BLOG (May 27, 2021), <https://www.sconline.com/blog/post/2021/05/27/del-hc-whatsapp-challenges-intermediary-rules-says-traceability-will-break-end-to-end-encryption-breach-privacy-union-of-india-says-no-fundamental-right-is-absolute/>.
65. SFLC.in, SFLC.in Analysis of X Corp v Union of India Judgement (2025), <https://sflc.in/xcorp-judgment-analysis/>.