INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE THREE GENERATIONS OF INDIAN CYBER LAW: ANALYZING THE SHIFT FROM COMMERCE TO CRIME CONTROL TO RIGHTS-BASED GOVERNANCE

AUTHOR – AKSHITA TRIPATHI* & DR. KAVYA CHANDEL**

* STUDENT AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

** ASSISTANT PROFESSOR OF LAW AT AMITY LAW SCHOOL LUCKNOW, AMITY UNIVERSITY UTTAR PRADESH LUCKNOW CAMPUS

BEST CITATION – AKSHITA TRIPATHI & DR. KAVYA CHANDEL, THE THREE GENERATIONS OF INDIAN CYBER LAW: ANALYZING THE SHIFT FROM COMMERCE TO CRIME CONTROL TO RIGHTS-BASED GOVERNANCE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (4) OF 2026, PG. 333-347, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

This paper provides a comprehensive chronological and thematic analysis of the evolution of India's cyber legal framework, tracing its development from the unregulated early internet era of the 1990s to the complex data governance regimes of 2023. By examining legislative texts, judicial pronouncements, and institutional mechanisms, the study explores the trajectory of the Information Technology (IT) Act, 2000, and its subsequent regulatory amendments. The core argument posits that Indian cyber law has undergone a three-stage transition: beginning as a "first-generation" commerce-enabling framework primarily driven by the need to legitimize e-commerce, evolving into a "second-generation" crime-control and security-oriented regime following the 2008 amendments, and currently shifting towards a "third-generation" rights-based data governance architecture marked by the Digital Personal Data Protection Act (DPDPA) 2023. Key themes explored include the shifting paradigms of intermediary liability and "Safe Harbour" protections, the jurisprudential complexities of electronic evidence admissibility under Section 65B of the Indian Evidence Act, and the expansion of state surveillance and regulatory compliance mechanisms. Ultimately, this legal evolution reflects a broader global movement from "cyber-libertarianism" to "cyber-sovereignty," highlighting India's ongoing efforts to balance technological innovation, national security, and citizen rights in the digital age.

Keywords: Indian Cyber Law, Information Technology Act, 2000, Intermediary Liability, Data Governance, Cyber-Sovereignty

Introduction

The trajectory of cyber law in India reflects a complex interplay among rapid technological proliferation, economic liberalisation, and the reactive evolution of state capacity to regulate the digital domain. This chapter provides an exhaustive chronological and thematic analysis of India's cyber legal framework, tracing its genesis from the unregulated early internet era of the 1990s to the comprehensive data governance regimes of 2023. By examining legislative texts, judicial pronouncements, and institutional mechanisms, this chapter argues that Indian cyber law has transitioned from a purely commerce-enabling framework (first generation) to a crime-control and security-oriented regime (second generation), and finally towards a rights-based data governance architecture (third generation). This evolution mirrors the global shift from "cyber-libertarianism," in which the internet was viewed

as a space separate from the state, to "cyber-sovereignty," in which digital spaces are tightly integrated into national legal structures.

1.1 Pre-2000 Context: Early Internet Adoption and the Regulatory Vacuum

The decade preceding the enactment of the Information Technology Act, 2000, was characterised by a "wild west" environment in India's digital landscape. While the internet was officially launched for public use in India on August 15, 1995, by Videsh Sanchar Nigam Limited (VSNL), the legal infrastructure remained firmly rooted in the physical world of the 19th and early 20th centuries.[679] The period from 1995 to 2000 was marked by a stark disconnect between the burgeoning digital reality and the analogue legal system, creating significant friction in commerce, criminal investigation, and intellectual property protection.

1.1.1 The Arrival of Connectivity and the Infrastructure Monopoly

Before 1995, internet access in India was restricted to the educational and research community through the ERNET (Education and Research Network) project, initiated in 1986. This network was academic in nature, devoid of commercial transactions, and thus operated largely outside the purview of commercial law. The commercial launch in 1995 marked a paradigm shift, yet infrastructure limitations and state monopoly hamstrung it. VSNL, a government-owned entity, held exclusive control over international internet gateways, creating a bottleneck that not only limited bandwidth but also centralised control over content and access.[680]

During this nascent phase, the "dot-com" boom was reshaping global markets. Indian software companies began to integrate into the global value chain, providing back-office support and software development services. However, domestic internet penetration was low, and the user base was primarily among the elite and urban residents. The primary legal concerns of this era were not data privacy or surveillance, but rather connectivity, tariff regulation, and the dismantling of the VSNL monopoly to allow private Internet Service Providers (ISPs) to operate. It was only in November 1998 that the government ended VSNL's monopoly, paving the way for private ISPs and a subsequent explosion in internet usage.

This period witnessed a critical legal void: there was no recognition of electronic contracts, no validity for digital signatures, and no specific mechanism to address digital fraud. Businesses operated under the looming risk that their electronic records would be inadmissible in court under the Indian Evidence Act, 1872, which predated the digital era by over a century and relied heavily on "primary evidence" in the form of physical documents.[681]

1.1.2 Early Cyber Crimes and the Inadequacy of Traditional Law

The absence of a specialised cyber statute did not mean the absence of cybercrime. In the late 1990s, the first generation of digital offences emerged in India, which law enforcement agencies sought to fit within the Procrustean bed of the Indian Penal Code (IPC), 1860. These early cases served as litmus tests for the judiciary, underscoring the urgent need for specialised legislation.

One of the earliest and most illustrative cases was *Yahoo! Inc. v. Akash Arora* (1999).[682] In this instance, the defendant registered the domain name "yahooindia.com," which is identical to the plaintiff's famous trademark "Yahoo!". Since there was no specific legislation governing domain name squatting or cyber trademarks, the Delhi High Court had to rely on the traditional common law principle of "passing off." The Court issued a permanent injunction restraining the defendant, effectively

[679] Pavan Duggal, *Cyber Law: The Indian Perspective* (Saakshar Law Publications, New Delhi, 2002).
[680] "History of Internet in India", *available at*: https://en.wikipedia.org/wiki/Internet_in_India (last visited Jan. 18, 2026).
[681] The Indian Evidence Act, 1872 (Act 1 of 1872), ss. 61-65.
[682] *Yahoo! Inc. v. Akash Arora*, 1999 (19) PTC 201 (Del).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

recognising that the reputation of a service rendered on the internet is entitled to protection equivalent to that of a physical business. The judgment was landmark because it established that the "virtual" world was not a lawless zone and underscored that judges were compelled to extend analogical concepts to fit digital realities.

Similarly, the *Sony Sambandh* case highlighted jurisdictional and substantive gaps in the law of theft.[683] In this case, a Non-Resident Indian (NRI) ordered a Sony television online for a recipient in India using a stolen credit card. The delivery was made, and the fraud was discovered later. The Central Bureau of Investigation (CBI) registered the case under IPC Sections 418, 419, and 420 (Cheating). While a conviction was eventually secured, the case demonstrated the procedural nightmare of prosecuting digital fraud. "Data theft" or "identity theft" had to be laboriously reconstructed as "cheating" or "misappropriation of property" to fit existing IPC definitions. The concept of "computer resource" as a target of crime was missing, forcing prosecutors to focus on the *result* (loss of a TV) rather than the *act* (hacking/unauthorised access).

Another notorious example from this era was the "Euro Lottery" scam involving Kola Venkata Krishna Mohan in Andhra Pradesh.[684] He allegedly forged an email purporting to show that he had won a substantial Euro lottery, using this fabrication to defraud banks and individuals. The police had to rely on traditional forgery and cheating provisions, struggling to prove the authenticity of the electronic record (the email) in the absence of a specialised evidence law.

1.1.3 The Catalyst for Regulation: E-Commerce and NASSCOM's Role

Contrary to popular belief, the primary driver for the enactment of the IT Act 2000 was not cybercrime, but commerce. The National Association of Software and Service Companies (NASSCOM) lobbied heavily for a legal framework that would legitimise e-commerce.[685] As Indian IT companies moved up the value chain from body-shopping to providing business process outsourcing (BPO) and software solutions, their global clients demanded legally enforceable electronic contracts and assurances of data security.

The lack of legal recognition for electronic records was a non-tariff barrier to trade. If a contract signed digitally in Bangalore could not be enforced in a court in New York or London because Indian law did not recognise the signature, the business model of the entire IT sector would be at risk. Consequently, the Ministry of Commerce and the Ministry of Information Technology collaborated to draft legislation that would provide a "legal wrapper" for digital transactions.[686]

1.1.4 International Influence: UNCITRAL Model Law (1996)

Internationally, the United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996. This document became the blueprint for India's IT Act. The Model Law established two fundamental legal principles that India sought to domesticate:

1. **Functional Equivalence:** Electronic records should not be denied legal effect, validity, or enforceability solely because they are in electronic form.[687] An electronic contract should be treated as functionally equivalent to a paper contract.
2. **Media Neutrality:** The law should not discriminate between different forms of technology used to transmit information.[688] (However, as we shall see,

[683] *State v. Arif Azim*, Case No. 223/2018 (CBI); see also "First Cyber Crime Conviction", *available at*: https://www.cyberralegalservices.com (last visited Jan. 18, 2026).
[684] *State of A.P. v. Kola Venkata Krishna Mohan*, (unreported, see *CAG Report on Cyber Crimes*, Vol II, p. 1).
[685] NASSCOM, "The IT Act 2000: A NASSCOM Perspective", *available at*: https://nasscom.in (last visited Jan. 18, 2026).
[686] Ministry of Commerce, Government of India, *Report on Electronic Commerce* (1999).
[687] UNCITRAL Model Law on Electronic Commerce, 1996, art. 5.
[688] *Id.*, art. 9.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

India's 2000 Act failed on this count by favouring specific digital signature technology).

The *High-Powered Committee on Electronic Commerce* (1998), constituted by the government, further emphasised the need for tax neutrality and legal certainty.[689] The committee examined whether e-commerce transactions required a new tax regime. It concluded that while the *mode* of commerce had changed, the *substance* (income generation) remained the same, recommending that existing tax laws be adapted rather than rewritten, a stance that reflected the "neutrality" principle of the OECD.

1.1.5 Early Censorship and the Dawn of Blocking

The pre-2000 era also established the precedent for state censorship of the internet, often exercised without apparent statutory authority. During the 1999 Kargil War, the Dawn website was blocked by VSNL. This blocking was carried out without a specific statutory provision authorising digital censorship, relying instead on the state's monopoly control over the international telecommunications gateway. This ad-hoc executive action revealed a dangerous lack of procedural safeguards for free speech online, a theme that would haunt Indian cyber law for decades and eventually lead to the *Shreya Singhal* litigation.[690]

1.2 Information Technology Act, 2000: The Foundational Framework

The Information Technology Act, 2000 (IT Act), enacted on June 9, 2000, and notified on October 17, 2000, was India's legislative response to the digital revolution. It was a "first-generation" cyber law, primarily designed to facilitate e-commerce rather than to serve as a comprehensive penal code for the internet. It marked India as the 12th nation in the world to adopt a specific cyber law.[691]

1.2.1 Objectives and UNCITRAL Alignment

The Statement of Objects and Reasons of the IT Act explicitly references the UNCITRAL Model Law.[692] The preamble states the Act is to provide "legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication." This focus on *recognition* rather than *regulation* is key to understanding the character of the 2000 Act.

The Act achieved its enabling objectives through three core mechanisms:

1. **Legal Recognition of Electronic Records (Section 4):** It mandated that where any law required information to be in writing, that requirement is satisfied if the information is available in an electronic form and accessible for future reference. This provision effectively digitised the Statute of Frauds requirements in Indian law.[693]
2. **Legal Recognition of Digital Signatures (Section 5):** It gave digital signatures the same legal status as handwritten signatures. Crucially, the 2000 Act was *technology-specific*, recognising only asymmetric cryptographic systems (Public-Key/Private-Key) and hash functions. This was a deviation from the UNCITRAL principle of technology neutrality, a deviation that India would not correct until 2008.[694]
3. **Electronic Governance (Section 6):** It laid the foundation for "e-Governance" by allowing the filing of forms, applications, and payments to the government in electronic formats.[695] This section was visionary, anticipating the Digital India stack by over a decade.

[689] Ministry of Finance, *Report of the High Powered Committee on Electronic Commerce and Taxation* (2001).
[690] "Internet Censorship in India", *available at*: https://en.wikipedia.org/wiki/Internet_censorship_in_India (last visited Jan. 18, 2026).
[691] The Information Technology Act, 2000 (Act 21 of 2000).
[692] *Id.*, Statement of Objects and Reasons.
[693] *Id.*, s. 4.
[694] *Id.*, s. 5.
[695] *Id.*, s. 6.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 4 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1.2.2 Key Provisions: Data Protection and Privacy (Sections 43 & 72)

In the 2000 version of the Act, data protection was not a central theme. However, two sections provided nascent protections for data security and confidentiality.

- **Section 43 (Penalty for Damage to Computer, Computer System, etc.):** This section created a civil liability for unauthorised access. It listed contraventions, including downloading data, introducing viruses, or disrupting networks, without the owner's permission.
    - *Significance*: It introduced the concept of "statutory damages" (compensation) for data theft. If a hacker stole proprietary data, the victim could sue for damages up to ₹1 crore (initially). This was a remedy distinct from criminal prosecution.[696]
- **Section 72 (Penalty for Breach of Confidentiality and Privacy):** This was the sole privacy-focused criminal provision. It punished any person who, having secured access to electronic records *under the powers conferred by the Act*, disclosed that information without consent.[697]
    - *Limitation*: The scope was extremely narrow. It primarily applied to government officials (such as the Controller of Certifying Authorities) or to those exercising statutory powers. It did not cover private entities or general ISPs breaching user privacy, a gap that would be exploited in the BPO frauds of the mid-2000s.

1.2.3 Institutional Architecture: The Adjudicating Officer

A distinct and innovative feature of the IT Act was the creation of a quasi-judicial adjudicatory mechanism for civil contraventions, aiming to bypass the gridlocked civil courts.

The Adjudicating Officer (Section 46):

Section 46 empowered the Central Government to appoint an "Adjudicating Officer" (AO), typically a bureaucrat (Secretary of IT of a State), to hold inquiries into contraventions under Section 43.[698]

- **Jurisdiction:** The AO had the jurisdiction to adjudicate matters where the claim for injury or damage did not exceed ₹5 crore.
- **Powers:** The AO was vested with the powers of a Civil Court, including summoning witnesses, demanding evidence on affidavit, and ordering discovery.
- **Critique:** While theoretically sound, the mechanism suffered from severe implementation deficits. Many states delayed the appointment of AOs for years. Furthermore, the AOs were often bureaucrats without judicial training or technical expertise, resulting in low disposal rates and questionable judgment quality. The *Sol Infotech* case highlights the complexities AOs face in determining liability in phishing cases where the "intermediary" defence is raised.[699]

The Cyber Regulations Appellate Tribunal (CRAT):

Appeals from the Adjudicating Officer and the Controller of Certifying Authorities (CCA) are heard by the Cyber Regulations Appellate Tribunal (CRAT), later renamed the Cyber

[696] *Id.*, s. 43.
[697] *Id.*, s. 72.
[698] *Id.*, s. 46
[699] *Sol Infotech Pvt. Ltd. v. The Secretary, IT Department*, TDSAT Cyber Appeal No. 6/2014.

Appellate Tribunal (CyAT). This specialised tribunal was meant to be the final fact-finding authority on technical cyber matters. However, for extended periods (2011-2017), the tribunal remained non-functional due to the government's failure to appoint a Chairperson, rendering the appellate remedy illusory.[700]

1.2.4 Certifying Authorities (CAs) and the Controller (CCA)

To manage the digital signature ecosystem, the Act established the **Controller of Certifying Authorities (CCA)**. The CCA was tasked with licensing and regulating "Certifying Authorities" (such as TCS, SafeScrypt, and NIC) entities that are authorised to issue digital signature certificates to users. This hierarchical trust model (Root CA -> Licensed CA -> Subscriber) was directly imported from the PKI (Public Key Infrastructure) standards of the time. The CCA acts as the "Root of Trust" for India's digital signature framework.[701]

1.2.5 Critique of the 2000 Framework

While the IT Act 2000 was a landmark statute, it suffered from "technological tunnel vision."

1. **Lack of Privacy:** It lacked a comprehensive data protection regime. Section 72 was too narrow, and Section 43 was purely compensatory.
2. **Rigid Technology:** It recognised *only* digital signatures based on crypto-pairs, ignoring biometric authentication or simple electronic signatures, which hindered mass adoption.
3. **Weak Intermediary Protection:** The original Section 79 was ambiguous regarding the liability of platforms (ISPs, websites) for third-party content. It conditioned immunity on the intermediary having "no knowledge," a high bar that exposed CEOs to arrest, as seen in the *Baazee.com* case.[702]

1.3 Amendments and Rules: The 2008 Paradigm Shift and Beyond

The rapid proliferation of the internet, the explosion of mobile telephony, and the emergence of social media exposed the inadequacies of the 2000 Act. Two specific triggers necessitated a major overhaul: the *Baazee.com* case (2004) and the 2008 Mumbai Terror Attacks.

1.3.1 The *Baazee.com* Catalyst (Avnish Bajaj v. State)

In 2004, a clip containing sexually explicit content (the infamous "DPS MMS") was listed for sale on Baazee.com, an online auction site owned by eBay. The Delhi Police arrested Avnish Bajaj, the CEO of Baazee.com, charging him under Section 67 of the IT Act (Obscenity) and various IPC sections. The police argued that as the platform owner, he was vicariously liable for the content sold on his site.

The Delhi High Court, and later the Supreme Court, had to determine whether an intermediary could be held criminally liable for content uploaded by a third party without the intermediary's active participation or specific knowledge.[703] The arrest of a high-profile corporate executive sent shockwaves through the Indian IT and BPO industry. NASSCOM and legal experts argued that if platforms were held strictly liable for every instance of user-generated content, the business model of the internet would collapse. This case highlighted the inadequacy of the original Section 79 and prompted the development of a "Safe Harbour" regime.[704]

1.3.2 The Information Technology (Amendment) Act, 2008

Passed in December 2008 (shortly after the Mumbai attacks) and notified on October 27, 2009, this amendment fundamentally transformed the IT Act from a commerce

[700] "Cyber Appellate Tribunal defunct for years", *The Economic Times*, May 15, 2016.
[701] The Information Technology Act, 2000, s. 17.
[702] *Avnish Bajaj v. State (NCT of Delhi)*, (2005) 116 DLT 427.
[703] *Avnish Bajaj v. State (NCT of Delhi)*, (2008) 150 DLT 769.
[704] NASSCOM, "Intermediary Liability: The Indian Context" (2006).

statute to a comprehensive cyber-penal code.[705]

Key Legislative Changes

1. **Expansion of "Cyber Crimes" (Section 66A - 66F):** The amendment introduced a plethora of new offences to mirror the IPC but in the digital domain, addressing the gaps exposed by evolving criminal methodologies:
    - **Section 66A:** Punishment for sending "offensive" messages. This section was widely criticised for its vagueness ("grossly offensive," "menacing") and was eventually struck down by the Supreme Court in *Shreya Singhal* (2015).[706]
    - **Section 66C:** Identity theft, punishable by up to 3 years imprisonment.
    - **Section 66D:** Cheating by personation using a computer resource, covering phishing scams.
    - **Section 66E:** Violation of privacy, specifically voyeurism (capturing/publishing private images), filling the gap for image-based abuse.
    - **Section 66F:** Cyber Terrorism. This was a direct response to the use of technology in terror attacks. It criminalised acts committed with the intent to threaten the unity, integrity, security, or sovereignty of India, including denial of access to computer resources or unauthorised access to data. It carries a life sentence.[707]
2. **Data Protection and Corporate Liability (Sections 43A and 72A):**
    - **Section 43A (Compensation for failure to protect data):** This was a revolutionary addition. It mandated that any "body corporate" possessing "sensitive personal data or information" (SPDI) must implement "reasonable security practices." If negligence in maintaining these practices caused wrongful loss to a person, the body corporate was liable to pay *unlimited* damages (removing the ₹1 crore cap of Section 43). This effectively introduced a statutory tort for data breaches.[708]
    - **Section 72A (Punishment for Disclosure):** This section criminalised the disclosure of personal information obtained under a lawful contract without the consent of the person concerned. This was explicitly drafted to address "call centre fraud" scenarios in which employees sold customer data.[709]
3. **Technological Neutrality:** The amendment replaced the term "Digital Signature" with "Electronic Signature" throughout the Act. This enabled the government to adopt authentication technologies beyond asymmetric cryptographic systems (e.g., Aadhaar-based e-Sign), thereby broadening the scope of legally valid electronic authentication.[710]
4. **Safe Harbour 2.0 (Section 79): The amendment completely rewrote Section 79 to codify the "Safe Harbour"** principle. It explicitly stated that intermediaries are *not liable* for third-

[705] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009).
[706] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[707] Information Technology Act, 2000 (as amended), s. 66F.
[708] *Id.*, s. 43A.
[709] *Id.*, s. 72A.
[710] *Id.*, s. 3A.

party information, data, or communication links made available or hosted by them, provided they:

- Function limited to providing access.
- Do not initiate the transmission, select the receiver, or modify the information.
- Observe "due diligence" as prescribed by the Central Government.

This was the legislative "fix" for the *Avnish Bajaj* issue, protecting platforms such as Google, Facebook, and ISPs from liability for user actions.[711]

5. **Surveillance and Blocking (Sections 69 & 69A):** The amendment significantly expanded the state's power to intercept, monitor, and decrypt information (Section 69) and to block public access to any information through any computer resource in the interest of sovereignty and integrity of India (Section 69A). Section 69A has become the primary legal instrument for banning websites and applications (e.g., the 2020 ban on Chinese apps).[712]

1.3.3 The Rules of 2011: Defining "Due Diligence"

To operationalise the 2008 amendments, the government issued key regulations in 2011, which defined the contours of compliance for the next decade.

Information Technology (Intermediaries Guidelines) Rules, 2011

These rules defined the "due diligence" an intermediary must exercise to enjoy Section 79 immunity. They required intermediaries to:

- Publish a Privacy Policy and User Agreement.
- Prohibit users from hosting specific types of harmful content (e.g., defamatory, obscene, invasive of privacy).
- Remove content within 36 hours of receiving "actual knowledge" of its illegality. The interpretation of "actual knowledge" later became a contentious issue, settled by the Supreme Court in *Shreya Singhal*, which read it down to mean knowledge via a court order or government notification.[713]

The SPDI Rules, 2011

The *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011* (SPDI Rules) were framed under Section 43A.[714] They defined "Sensitive Personal Data" to include passwords, financial information, health conditions, sexual orientation, and biometric information. The rules mandated:

- Obtaining written consent before collection.
- Publishing a privacy policy.
- Allowing users to review and correct information.
- Appointing a Grievance Officer.

These rules constituted India's de facto privacy law until the enactment of the DPDPA in 2023.

1.3.4 The 2021 Intermediary Rules: A New Era of Regulation

In February 2021, the Ministry of Electronics and IT (MeitY) notified the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. These rules replaced the 2011 Intermediary Guidelines and represented a paradigm shift from "passive" to "active" regulation of Big Tech.[715]

[711] *Id.*, s. 79.
[712] *Id.*, ss. 69, 69A.
[713] *Shreya Singhal*, *supra* note 28, at para 119.
[714] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[715] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 4 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Comparison: IT Rules 2011 vs. IT Rules 2021

The 2021 Rules introduced a tiered structure and significantly higher compliance burdens, particularly for large platforms.

Feature	IT Rules 2011	IT Rules 2021
Classification of Intermediaries	No distinction based on size or user base. All intermediaries are treated equally.	Introduced a new category: **"Significant Social Media Intermediaries" (SSMIs)**. SSMIs are platforms with registered users in India above a threshold (notified as 5 million).
Personnel Requirements	Required only the appointment of a Grievance Officer.	SSMIs must appoint a **Chief Compliance Officer**, a **Nodal Contact Person** (for 24x7 law enforcement coordination), and a **Resident Grievance Officer**. Crucially, all these officers **must be residents of India**.
Traceability (First Originator)	No such requirement existed.	SSMIs providing messaging services (e.g., WhatsApp) must enable the identification of the **"first originator"** of information for serious offences (sovereignty, child sexual abuse, rape). This "Traceability" clause is currently challenged in courts on privacy grounds.[716]
Content Takedown Timelines	Remove content within 36 hours of "actual knowledge."	Retains the 36-hour rule generally, but mandates removal within **24 hours** for content depicting non-consensual nudity or sexual acts.
Scope (OTT & News)	Did not cover digital news or OTT platforms.	Expanded the ambit to regulate **Digital News Publishers** and **OTT Platforms** (e.g., Netflix, Amazon Prime) under a Code of Ethics and a three-tier grievance redressal mechanism (Self-regulation -> Industry Body -> Government

[716] *Id.*, Rule 4(2).

		Oversight).
User Verification	No requirement.	SSMIs must provide a mechanism for users to voluntarily verify their accounts (e.g., via Blue Ticks).

The 2021 Rules effectively ended the era of the "passive conduit," forcing platforms to build local capacity for enforcement and grievance redressal. The inclusion of digital news and OTT under the IT Act rules was also legally significant, as it asserted executive control over content that had previously been unregulated or regulated under different statutes.

1.4 Related Legislation: The Intersection of Codes

Cyber law in India operates in a symbiotic relationship with traditional penal and procedural codes. The IT Act often functions as a special law that overrides general law. Still, the provisions of the Indian Penal Code (IPC) and the Indian Evidence Act (IEA) are frequently invoked concurrently.

1.4.1 IPC and Cyber Fraud: The "420" Application

While the IT Act addresses specific technical offences (such as hacking or theft of source code), the IPC remains the primary instrument for economic crimes committed through digital means.

- **Section 420 (Cheating and dishonestly inducing delivery of property):** This section is extensively used for online financial fraud, phishing, and "Nigerian Prince" (419) scams.[717] The courts have held that the medium of the fraud (e.g., internet or email) does not alter the nature of the crime. If the ingredients of "deception" and "dishonest inducement" causing the victim to deliver property (money) are met, Section 420 applies. This allows police to invoke the stricter non-bailable provisions of the IPC alongside the bailable offences under the IT Act (such as Section 66).
- **Overlap and Double Jeopardy:** In *Sharat Babu Digumarti v. Govt of NCT of Delhi* (2017), the Supreme Court clarified the interplay between the IPC and the IT Act regarding obscenity. It held that since the IT Act (Section 67) is a special law dealing with electronic obscenity, it overrides the general IPC provision (Section 292). If an accused is acquitted under the IT Act, they cannot be prosecuted under the IPC for the same electronic act. This affirmed the principle *generalia specialibus non derogant* (general things do not derogate from extraordinary things).[718]

1.4.2 The Evidence Act and the Saga of Section 65B

The admissibility of electronic records has been one of the most litigated and jurisprudentially complex aspects of Indian cyber law. The IT Act, 2000, amended the Indian Evidence Act, 1872, by inserting **Section 65B**, a special provision governing the admissibility of electronic records as secondary evidence.

The evolution of judicial interpretation of Section 65B reflects the struggle to balance the "ease of proving" evidence with the need to ensure its "authenticity" in an era of deepfakes and easy manipulation.

1. The "Navjot Sandhu" Era (2005 - 2014): Laxity

In *State (NCT of Delhi) v. Navjot Sandhu* (2005), dealing with the Parliament Attack case, the Supreme Court held that the requirement of a certificate under Section 65B(4) was *not* mandatory.[719] The Court ruled that electronic records could be proved through oral evidence or under the general secondary evidence provisions (Sections 63 and 65) of the Evidence

[717] The Indian Penal Code, 1860 (Act 45 of 1860), s. 420.

[718] *Sharat Babu Digumarti v. Govt. of NCT of Delhi*, (2017) 2 SCC 18.

[719] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.

Act. This meant that printouts of call records could be admitted without a specific certificate from the telecommunications provider attesting to the server's integrity. This ruling was criticised for ignoring the "special" nature of digital evidence and the legislative intent behind Section 65B.

2. The "Anvar P.V." Correction (2014): Strict Compliance

In *Anvar P.V. v. P.K. Basheer* (2014), a three-judge bench of the Supreme Court explicitly overruled *Navjot Sandhu*. It held that Section 65B is a "complete code" for electronic evidence.[720] The Court ruled that a certificate under **Section 65B(4),** which certifies that the computer output was produced by a computer used regularly, that it was functioning correctly, and that the data is a reproduction of the original, is a **mandatory condition precedent** for the admissibility of any secondary electronic evidence (like printouts, CDs, or USB drives). Without this certificate, electronic evidence is strictly *inadmissible*. This judgment restored the sanctity of the statutory safeguard.

3. The "Shafhi Mohammad" Dilution (2018): Confusion

In *Shafhi Mohammad v. State of H.P.* (2018), a two-judge bench attempted to dilute the strictness of *Anvar*. It ruled that the certificate requirement could be relaxed if the party producing the evidence did not have the device (e.g., a citizen producing CCTV footage from a shop).[721] It characterised the requirement as "procedural" rather than substantive, creating confusion in trial courts as to whether the certificate was truly mandatory.

4. The "Arjun Panditrao" Finality (2020): Settled Law

The controversy was finally settled by a massive three-judge bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020).[722] The Court reaffirmed *Anvar P.V.* and overruled *Shafhi Mohammad*.

- **Holding:** The Section 65B(4) certificate is a **mandatory** condition precedent for admissibility. Oral evidence cannot substitute for it.
- **Remedy for Non-Possession:** If a party (e.g., a victim) cannot obtain the certificate (e.g., from a telecom company or Facebook), they must apply to the trial judge to exercise their powers under the Evidence Act or CrPC to summon the certificate from the relevant authority. The Court cannot simply waive the requirement; it must compel the production of the certificate.
- **Direction:** The Court also issued general directions to cellular companies and ISPs to maintain records in a segregated and secure manner to facilitate the issuance of these certificates.

This trajectory from *Navjot Sandhu* to *Arjun Panditrao* demonstrates the judiciary's increasing sophistication in understanding the nuances of digital evidence integrity.

1.5 Institutional Framework: The Enforcers

The implementation of cyber laws in India is driven by a specialised institutional architecture that is evolving to meet the scale of the digital challenge.

1.5.1 Ministry of Electronics and Information Technology (MeitY)

MeitY is the nodal ministry for all policy matters relating to IT, electronics, and the internet. Established as a separate Ministry in 2016, it is the primary rule-making authority for the IT Act.[723] MeitY houses key divisions for Cyber Laws, E-Governance, and Cyber Security. It is responsible for issuing regulations (e.g., the 2021 Intermediary Rules) and for administering the Digital India programme. Its role has shifted from promoting the IT industry (through the

[720] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[721] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
[722] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[723] Government of India (Allocation of Business) Rules, 1961 (as amended).

Department of Electronics) to regulating the digital commons.

1.5.2 CERT-In (Indian Computer Emergency Response Team)

Established under Section 70B of the IT Act (inserted in 2008), CERT-In is the national nodal agency for cyber security incident response.

- **Mandate:** Its functions include the collection, analysis, and dissemination of information on cyber incidents, and issuing emergency measures and guidelines.[724]
- **2022 Directions Controversy:** In April 2022, CERT-In issued new "Directions" under Section 70B(6) that significantly expanded the surveillance and reporting obligations of private entities.[725]
    - **Reporting Timeline:** Mandatory reporting of cyber incidents (breaches, ransomware) within **6 hours** of noticing them.
    - **Logs:** All service providers and data centres must maintain logs of ICT systems for a rolling period of **180 days**.
    - **VPN Regulation:** Virtual Private Network (VPN) providers were mandated to maintain user logs (names, IPs, usage patterns) for 5 years. This effectively banned "no-log" VPNs in India, compelling major providers such as NordVPN and ExpressVPN to shut down their physical Indian servers.[726] While the government justified this as necessary to trace cybercriminals and terrorists, privacy advocates criticised it as excessive surveillance that undermined the very purpose of privacy tools.

1.5.3 Cyber Appellate Tribunal (CyAT) to TDSAT

As discussed in Section 4.2.3, the IT Act created the **Cyber Appellate Tribunal (CyAT)** to hear appeals from the Adjudicating Officer (AO).

- **The Vacuum:** For a prolonged period (2011-2017), the CyAT was dysfunctional due to the non-appointment of a Chairperson. This meant that even if an AO passed an order, the aggrieved party had nowhere to appeal, effectively stalling the justice delivery mechanism.
- **The Merger (2017):** The Finance Act, 2017, rationalised tribunals and merged the CyAT with the **Telecom Disputes Settlement and Appellate Tribunal (TDSAT)**.[727] Currently, the TDSAT exercises appellate jurisdiction over cyber matters. While this resolved the vacancy issue, data indicate that the disposal rate of cyber appeals remains slow relative to telecom disputes, and there is concern that overloading a telecom tribunal with technical cyber matters dilutes the specialised focus required for cyber jurisprudence.

1.6 Timeline of Evolution

The following table synthesises the critical milestones in the evolution of India's cyber legal regime, highlighting the shift from commerce to control to rights.

Year	Milestone	Key Development / Legal Shift
1998	**Policy Genesis**	High-Powered Committee on E-Commerce recommends tax neutrality. NASSCOM lobbies for IT law to boost exports. Monopoly of VSNL ends.

[724] Information Technology Act, 2000, s. 70B.
[725] CERT-In, "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000", No. 20(3)/2022-CERT-In (Apr. 28, 2022).
[726] "CERT-In Directions: Impact on VPNs", *Internet Freedom Foundation*, May 2022.
[727] The Finance Act, 2017 (Act 7 of 2017), Part XIV

2000	**IT Act Enacted**	**The Information Technology Act, 2000, was** passed. Focus on e-commerce, legal recognition of electronic records (S. 4), digital signatures (S. 5). Created Adjudicating Officer (S. 46).
2004	**Baazee.com Case**	CEO Avnish Bajaj arrested for user content. Highlights the lack of "Safe Harbour" for intermediaries—triggers amendment discussions.
2005	**Navjot Sandhu**	Supreme Court rules Section 65B certificate for electronic evidence is *not* mandatory (later overruled).
2008	**IT (Amendment) Act**	**Paradigm Shift:** Enacted post-Mumbai attacks. Added Cyber Terrorism (S. 66F), Data Protection (S. 43A), Safe Harbour (S. 79), and the controversial S. 66A.
2011	**IT Rules Notified**	"Due Diligence" guidelines for intermediaries; SPDI Rules (Privacy) enacted under S. 43A.
2014	**Anvar P.V. Judgment**	Supreme Court mandates Section 65B certificate for electronic evidence admissibility, overruling *Navjot Sandhu*.
2015	**Shreya Singhal Case**	Supreme Court strikes down **Section 66A** as unconstitutional for violating Freedom of Speech (Article 19(1)(a)).
2017	**Puttaswamy Judgment**	**Right to Privacy** declared a Fundamental Right (Article 21)—catalyst for a standalone data protection law.
2017	**Tribunal Merger**	The Cyber Appellate Tribunal (CyAT) was merged into the TDSAT under the Finance Act, 2017.
2018	**Srikrishna Committee**	Justice Srikrishna Committee submits report and draft Personal Data Protection Bill, proposing a GDPR-style law.
2020	**Arjun Panditrao**	Supreme Court settles Section 65B controversy; certificate is a mandatory condition precedent.
2021	**Intermediary Rules**	Concept of SSMI introduced; Traceability mandated; Regulation extended to OTT and Digital News.
2022	**CERT-In Directions**	6-hour reporting mandate; VPN logging requirements enforced; Synchronization of clocks.
2023	**DPDPA Enacted**	**Digital Personal Data Protection Act, 2023,** replaces Section 43A. Shift from compensation to a high-penalty compliance regime.

1.7 Conclusion: The Third Generation of Cyber Law

As India moves through the 2020s, the "Third Generation" of cyber law is taking shape. The enactment of the **Digital Personal Data Protection Act, 2023 (DPDPA),** marks a decisive break from the IT Act's limited privacy provisions (Section 43A).

A critical "third-order" insight is the shift in the philosophy of remedy. Under the old **Section 43A** regime, if a company was negligent in relation to data, it had to pay *compensation* directly to the victim. Under the new **DPDPA 2023**, if a Data Fiduciary breaches its duties, it shall pay a substantial *penalty* (up to ₹250 crore) to the Data Protection Board (the state). The victim is not entitled to compensation under the Act. This represents a shift from a tort-based (civil wrong/compensation) approach to a regulatory compliance (state penalty) approach.[728] While this incentivises companies to comply to avoid fines, it may disempower individual victims seeking redress.

Furthermore, the DPDPA introduces controversial government exemptions. Section 17(2) allows the government to exempt state agencies from the Act in the interests of sovereignty, security, and public order.[729] Unlike the GDPR (Article 23), which requires such exemptions to be "necessary and proportionate," the DPDPA's language is broader, raising concerns about potential unchecked state surveillance in the post-*Puttaswamy* era.[730]

Looking ahead, the proposed **Digital India Act** (DIA) is intended to replace the IT Act 2000 in its entirety. The DIA seeks to address challenges that 2000-era legislators could not have imagined: Artificial Intelligence, algorithmic accountability, deepfakes, and the regulation of "high-risk" AI systems. The evolution of cyber laws in India, therefore, is not a static history but a dynamic, ongoing process of keeping pace with the pace of digital transformation. From the VSNL monopoly to the AI age, the law continues to adapt, attempting to balance the triad of innovation, security, and citizen rights in the world's largest digital democracy.

[728] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 33.
[729] *Id.*, s. 17(2).
[730] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

BIBLIOGRAPHY

Table of Cases

- *Anvar P.V. v. P.K. Basheer* (2014).
- *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020).
- *Avnish Bajaj v. State* (Baazee.com Case) (2004).
- *Puttaswamy* Judgment (2017).
- *Shafhi Mohammad v. State of H.P.* (2018).
- *Sharat Babu Digumarti v. Govt of NCT of Delhi* (2017).
- *Shreya Singhal* Case (2015).
- *Sony Sambandh* Case.
- *State (NCT of Delhi) v. Navjot Sandhu* (2005).
- *Yahoo! Inc. v. Akash Arora* (1999).

Statutes, Acts, and Rules (India)

- Digital Personal Data Protection Act (DPDPA), 2023.
- Finance Act, 2017.
- Indian Evidence Act, 1872.
- Indian Penal Code (IPC), 1860.
- Information Technology Act, 2000.
- Information Technology (Amendment) Act, 2008.
- Information Technology (Intermediaries Guidelines) Rules, 2011.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules).

Committee Reports and Guidelines

- CERT-In Directions under Section 70B(6) (2022).
- High-Powered Committee on Electronic Commerce (1998).
- Justice Srikrishna Committee Report and Draft Personal Data Protection Bill (2018).

International Legal Documents

- General Data Protection Regulation (GDPR).
- United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996).