Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

INFORMATION TECHNOLOGY LAW IN INDIA: Regulation, Liability, Commerce & Protections Under the IT Act

Srinivas M.K.[1], Prof.(Dr.) Suresh M Benjamin[2]

[1]Ph.D. Scholar (Law), [2]Professor
Department of Studies in Law, University of Mysore,
University of Mysore

Abstract
This article analyzes the constitutional, statutory, and policy dimensions of information technology law in India, with a specific focus on the Information Technology Act, 2000 (as amended). It examines the Act's scope and objectives, criminal and security provisions, commercial and e-commerce regulation, intermediary-liability and internet governance, intellectual property challenges in the digital environment, adjudication of domain-name disputes, and emerging concerns like semiconductor technology protection. By situating the IT Act within the larger framework of digital governance and free speech jurisprudence, this article highlights ongoing legal challenges and the need for evolving legal frameworks suited to 21st-century technologies based on the Indian approach of regulation. This paper embarks on the point that though the Original IT Act of 2000 is having lacuna in not dealing with many forms of cyber crimes yet , the amendments incorporated to plug them through the IT (Amendment) Act 2008 which also broadened its scope by bringing under its ambit various forms of cyber-crimes.

Keywords: Information Technology Act; cybercrime; e-commerce; intermediary liability; intellectual property; domain name disputes; semiconductor protection; digital governance; India.

INTRODUCTION

The Information Technology Act, 2000 (IT Act) constitutes India's foundational statutory framework governing digital communications, electronic commerce, cybersecurity, and cyber-enabled offences.

[1] *Ph.D. Scholar (Law), Department of Studies in Law, University of Mysore, Gold Medallist in B.Sc. and M.Sc.; recipient of five Gold Medals and three Cash Prizes in LL.M. (Constitutional Law) with Distinction from the University of Mysore. He holds an Associateship and Diploma in Insurance from the Insurance Institute of India, Mumbai, is UGC-NET qualified, and is a multilingual scholar and practicing advocate.*

Orcid: https://orcid.org/0009-0002-0475-9447

Email: srinivasmk@law.uni-mysore.ac.in

[2] *Dean ,Faculty of Law, Chairman & Head of the Department of Studies in Law, University of Mysore*

Enacted at the turn of the millennium, the Act reflects India's early legislative response to the growing role of information technology in governance, trade, and social interaction. Its primary objective was to confer legal recognition upon electronic records and digital signatures, thereby enabling electronic transactions and facilitating e-governance initiatives.[3] In the Indian context, the Information Technology Act, 2000 remains a cornerstone of digital regulation, providing legal certainty to electronic transactions, enabling enforcement against cyber offences, and facilitating India's participation in the global digital economy. While the Act has demonstrated remarkable adaptability through judicial interpretation and legislative amendments, rapid technological developments—particularly in AI governance, platform regulation, and data protection—have exposed structural limitations. Consequently, the IT Act increasingly operates as a foundational but transitional statute, supplemented by newer digital laws and constitutional jurisprudence, while continuing to play a critical role in India's evolving techno-legal landscape.

Legislative Objectives and International Alignment

The IT Act was enacted pursuant to India's obligations to modernize its commercial laws in line with international best practices, particularly the UNCITRAL Model Law on Electronic Commerce (1996).[2] This harmonization objective is expressly reflected in the Act's recognition of functional equivalence between electronic and paper-based transactions. Sections 4 and 5 of the Act provide statutory recognition to electronic records and digital signatures, respectively, establishing that electronic documents and authentication methods shall not be denied legal validity solely on the ground that they are in electronic form.[4]

From a policy perspective, this alignment has been critical in integrating India into the global digital economy, particularly in sectors such as cross-border outsourcing, fintech, e-commerce, and cloud-based services. The Supreme Court has repeatedly acknowledged that the IT Act must be interpreted purposively to accommodate evolving technologies rather than restrict innovation.[5]

Territorial and Extraterritorial Application

A distinctive feature of the IT Act is its extraterritorial reach. Section 1(2), read with Section 75, extends the application of the Act to offences or contraventions committed outside India, provided that a computer, computer system, or computer network located in India is involved.[6] This provision assumes heightened relevance in the contemporary context of cloud computing, cross-border data flows, and transnational cybercrime.

Indian courts have affirmed that the legislature intentionally adopted a broad jurisdictional scope to address the borderless nature of cyberspace. In State of Maharashtra v. Mohd. Yakub, although predating the IT Act, the Supreme Court emphasized that economic and technological offences require expansive interpretative approaches to prevent regulatory evasion an approach later reflected in cyberlaw jurisprudence.[7]

[3] UNCITRAL Model Law on Electronic Commerce, G.A. Res. 51/162 (Dec. 16, 1996).

[4] Information Technology Act, No. 21 of 2000, §§ 4–5 (India).

[5] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

[6] Information Technology Act, No. 21 of 2000, §§ 1(2), 75 (India).

[7] *State of Maharashtra v. Mohd. Yakub*, A.I.R. 1980 S.C. 1111 (India).

Regulation of Electronic Contracts and E-Commerce

The IT Act plays a pivotal role in validating electronic contracts, which are now central to India's digital economy. Section 10A, inserted by the Information Technology (Amendment) Act, 2008, explicitly recognizes the validity of contracts formed through electronic means.[8] This provision has been judicially interpreted to place electronic contracts on equal footing with traditional contracts under the Indian Contract Act, 1872.

In Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., the Supreme Court held that contracts concluded via email exchanges are legally enforceable, provided that offer, acceptance, and intention to create legal relations are clearly established.[9] This interpretation has facilitated the exponential growth of online marketplaces, digital procurement systems, and algorithm-driven contracting mechanisms in India.

Cyber Offences, Data Security, and Emerging Technologies

The IT Act also establishes a comprehensive framework for addressing cyber offences, including unauthorized access (Section 43), hacking (Section 66), identity theft (Section 66C), and cyber terrorism (Section 66F).[10] The 2008 amendments significantly expanded the scope of offences to address evolving technological threats such as phishing, online fraud, and misuse of digital identities.

With the rapid adoption of artificial intelligence (AI), Internet of Things (IoT), and big data analytics, the relevance of Sections 43A and 72A has increased substantially. Section 43A imposes civil liability on body corporates that fail to implement "reasonable security practices" in protecting sensitive personal data, while Section 72A criminalizes unlawful disclosure of information in breach of lawful contracts.[11]

In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court recognized informational privacy as a fundamental right under Article 21 of the Constitution.[12]Although the IT Act predates this judgment, the Court explicitly acknowledged that existing data protection provisions under the IT Act were inadequate, thereby catalyzing subsequent legislative initiatives such as the Digital Personal Data Protection Act, 2023. Nonetheless, until sector-specific AI or cybersecurity legislation is enacted, the IT Act continues to function as the primary legal instrument governing digital misconduct and data-related liabilities.

Adjudicatory Mechanisms and Institutional Framework

The IT Act establishes specialized adjudicatory mechanisms, including Adjudicating Officers under Section 46 and the Cyber Appellate Tribunal (now merged into the Telecom Disputes Settlement and Appellate Tribunal).[13] These mechanisms were designed to ensure expeditious resolution of cyber disputes and reduce the burden on conventional courts. However, delays in appointments and procedural

[8] Information Technology (Amendment) Act, No. 10 of 2009, § 10A (India).
[9] *Trimex Int'l FZE Ltd. v. Vedanta Aluminium Ltd.*, (2010) 3 S.C.C. 1 (India).
[10] Information Technology Act, No. 21 of 2000, §§ 43, 66, 66C, 66F (India).
[11] Id. §§ 43A, 72A.
[12] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[13] Information Technology Act, No. 21 of 2000, §§ 46–48 (India).

inefficiencies have limited their effectiveness, prompting calls for institutional reform in light of increasing cyber litigation.

CRIMINAL AND SECURITY ASPECTS OF INFORMATION TECHNOLOGY IN INDIA

The criminal and security dimensions of the Information Technology Act, 2000 (IT Act) represent one of its most consequential regulatory functions. Recognizing the unique vulnerabilities of digital infrastructures, the Act establishes a layered framework of civil liability, criminal sanctions, and national security mechanisms to address cybercrime, data misuse, and threats to critical information infrastructure.

A. Statutory Framework of Cyber Offences

The IT Act criminalizes a broad spectrum of conduct involving unauthorized access to computer systems, data manipulation, identity fraud, and cyber-enabled threats to national security. Sections 65 to 74 (as amended) collectively define offences relating to tampering with computer source documents, hacking, publication of prohibited content, breach of confidentiality, and misuse of digital identities.[14]

Section 43 functions as the foundational civil liability provision, imposing compensation for unauthorized access, data theft, introduction of malware, denial of service attacks, or damage to computer systems.[15]This provision is technology-neutral and applies irrespective of criminal intent, making it particularly relevant in cases involving corporate data breaches and negligent cybersecurity practices.

Criminal liability is triggered under Section 66 when conduct described under Section 43 is committed dishonestly or fraudulently.[16] Subsequent amendments introduced specialized offences reflecting technological evolution:

a) Section 66C criminalizes identity theft, including fraudulent use of electronic signatures, passwords, or biometric identifiers.[17]
b) Section 66D addresses cheating by personation through computer resources, targeting online fraud and phishing schemes.[18]
c) Section 66F defines cyber terrorism, encompassing acts intended to threaten the sovereignty, integrity, security, or economic stability of India through digital means.[19]

Indian courts have emphasized that cyber offences, given their scale and anonymity, warrant stringent enforcement. In CBI v. Arif Azim, one of India's earliest cybercrime prosecutions, the court recognized

[14] ibid

[15] Id. § 43.

[16] Id. § 66.

[17] Id. § 66C.

[18] Id. § 66D.

[19] Id. § 66F.

the evidentiary reliability of electronic records and underscored the necessity of specialized cybercrime laws.[20]

B. Privacy, Surveillance, and State Powers

The IT Act also confers extensive surveillance and interception powers upon the State. Section 69 authorizes the Central or State Governments to intercept, monitor, or decrypt information transmitted through computer resources in the interests of sovereignty, national security, public order, or prevention of cognizable offences.[21] Complementary powers are granted under Sections 69A (blocking of public access to information) and 69B (monitoring of traffic data).

These provisions have generated sustained constitutional scrutiny due to their potential impact on privacy, free speech, and due process. The Supreme Court's landmark judgment in Shreya Singhal v. Union of India represents a pivotal moment in Indian cyberlaw jurisprudence. **The Court struck down Section 66A which criminalized the sending of "offensive" or "menacing" messages online as unconstitutionally vague and disproportionate, holding that it violated Article 19(1)(a) of the Constitution.**[22]

Importantly, while invalidating Section 66A, the Court upheld Sections 69A and the associated Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, on the ground that they contained procedural safeguards and were narrowly tailored to legitimate state interests.[23] This distinction illustrates the judiciary's attempt to balance national security imperatives with constitutional freedoms in cyberspace.

C. Cybersecurity and Institutional Mechanisms

Beyond criminalization, the IT Act adopts a preventive and institutional approach to cybersecurity. Section 70 empowers the government to designate Critical Information Infrastructure (CII), the destruction or disruption of which would have a debilitating impact on national security, the economy, or public health.[24]

To operationalize cybersecurity governance, the Act establishes specialized bodies:
Indian Computer Emergency Response Team (CERT-In) under Section 70B, responsible for incident response, vulnerability disclosure, and coordination during cyber incidents.[25]

National Critical Information Infrastructure Protection Centre (NCIIPC) under Section 70A, tasked with protecting critical digital assets such as power grids, financial systems, and telecommunications networks.[26]

[20] *CBI v. Arif Azim*, (2003) (unreported Delhi Dist. Ct.) (India).

[21] Information Technology Act, No. 21 of 2000, § 69 (India).

[22] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

[23] Id.

[24] Information Technology Act, No. 21 of 2000, § 70 (India).

[25] Id. § 70B.

[26] Id. § 70A.

In the context of emerging technologies such as cloud computing, artificial intelligence, and Internet of Things (IoT) ecosystems CERT-In's 2022 Directions mandating breach reporting within fixed timelines have significantly expanded compliance obligations for intermediaries and data handlers. These developments demonstrate how the IT Act continues to function as the backbone of India's cybersecurity regime, even as sector-specific regulations evolve.

D. Constitutionalization of Cybersecurity and Privacy

The Supreme Court's decision in Justice K.S. Puttaswamy (Retd.) v. Union of India constitutionalized the right to informational privacy under Article 21, fundamentally reshaping the interpretation of surveillance and data protection provisions under the IT Act.[27]The Court explicitly recognized that while national security is a legitimate state aim, any infringement of privacy must satisfy the tests of legality, necessity, and proportionality.

Consequently, the criminal and security provisions of the IT Act are no longer interpreted in isolation but are subject to constitutional scrutiny grounded in fundamental rights jurisprudence. This shift has influenced legislative developments, including the enactment of the Digital Personal Data Protection Act, 2023, while leaving the IT Act as the primary statute governing cyber offences and security enforcement.

The criminal and security architecture of the Information Technology Act, 2000 reflects India's attempt to address cyber threats through a combination of punitive sanctions, preventive regulation, and institutional oversight. While the Act has demonstrated adaptability in responding to cybercrime and national security concerns, judicial interventions particularly in Shreya Singhal and Puttaswamy have ensured that enforcement powers remain constitutionally bounded. In the contemporary technological landscape, the IT Act continues to operate as a central pillar of India's cybercrime and cybersecurity regime, even as its limitations necessitate complementary legislative frameworks.

COMMERCIAL ASPECTS OF INFORMATION TECHNOLOGY AND E-COMMERCE IN INDIA

The commercial dimension of the Information Technology Act, 2000 (IT Act) is central to India's digital economy, as it provides the legal infrastructure necessary for electronic commerce, online contracting, and digital authentication. By recognizing electronic records and digital signatures as legally valid, the Act removes formal barriers that traditionally impeded the use of electronic means in commercial transactions.

A. Legal Recognition of Electronic Records and Digital Signatures

Section 4 of the IT Act embodies the principle of functional equivalence, providing that where any law requires information to be in writing or in printed form, such requirement shall be deemed satisfied if the information is rendered or made available in an electronic form and remains accessible for subsequent reference.[28]This provision ensures that electronic documents such as online invoices, electronic purchase orders, and digital contracts cannot be denied legal effect solely on the ground of their digital nature.

[27] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).

[28] Information Technology Act, No. 21 of 2000, § 4 (India).

Complementing this, Section 5 accords legal recognition to digital signatures, stipulating that where a law requires authentication by signature, such requirement is fulfilled if the document is authenticated by a digital signature affixed in accordance with the Act.[29] Together, Sections 4 and 5 form the statutory backbone of enforceable online contracts in India, enabling e-commerce platforms, fintech companies, and digital service providers to conduct business without reliance on physical documentation.

Judicial interpretation has reinforced this commercial utility. In Trimex International FZE Ltd. v. Vedanta Aluminium Ltd., the Supreme Court held that contracts concluded through electronic communications, including email exchanges, are legally enforceable provided the essential elements of contract formation offer, acceptance, and intention to create legal relations are satisfied.[30] This decision has been instrumental in legitimizing click-wrap agreements, online procurement contracts, and digitally negotiated commercial arrangements.

B. Regulation of Digital Signatures and Certifying Authorities

To ensure trust and authenticity in electronic transactions, the IT Act establishes a comprehensive regulatory framework for Certifying Authorities (CAs) under Sections 17 to 34.[31] These authorities are licensed by the Controller of Certifying Authorities and are responsible for issuing Digital Signature Certificates (DSCs), which verify the identity of parties engaging in electronic transactions.

The regulatory oversight of CAs serves a critical commercial function by reducing transaction costs, mitigating identity fraud, and enhancing confidence in digital markets. In sectors such as e-tendering, corporate filings, securities trading, and cross-border commerce, DSCs operate as legally reliable substitutes for handwritten signatures. Courts have recognized the evidentiary value of digitally signed documents, subject to compliance with statutory standards and certification requirements.[32]

C. E-Commerce Platforms and Intermediary Obligations

E-commerce platforms in India operate within a complex regulatory environment shaped by the IT Act, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and consumer protection legislation. While the IT Act facilitates electronic contracting, it simultaneously imposes compliance obligations relating to cybersecurity, data protection, and unlawful content.

Section 79 of the IT Act provides conditional safe harbor protection to intermediaries, exempting them from liability for third-party content hosted on their platforms, provided they observe due diligence and do not knowingly aid or abet unlawful acts.[33]This provision is commercially significant, as it enables the scalability of online marketplaces while balancing accountability.

In Shreya Singhal v. Union of India, the Supreme Court clarified that intermediary liability under Section 79 is triggered only upon actual knowledge through a court order or government notification,

[29] Id. § 5.

[30] *Trimex Int'l FZE Ltd. v. Vedanta Aluminium Ltd.*, (2010) 3 S.C.C. 1 (India).

[31] Information Technology Act, No. 21 of 2000, §§ 17–34 (India).

[32] *State of Maharashtra v. Dr. Praful B. Desai*, (2003) 4 S.C.C. 601 (India).

[33] Information Technology Act, No. 21 of 2000, § 79 (India).

thereby preventing excessive private censorship and ensuring predictability for digital businesses.[34]This interpretation has been critical for the operational viability of large e-commerce platforms, social commerce intermediaries, and payment aggregators.

D. Secure Transactions, Consumer Trust, and Emerging Technologies

From a commercial perspective, the IT Act also indirectly regulates transactional security through provisions such as Section 43A, which imposes civil liability on body corporates for failure to implement reasonable security practices in handling sensitive personal data.[35] In the age of platform-based commerce, AI-driven pricing, and cloud-hosted payment systems, compliance with cybersecurity norms has become an essential component of commercial risk management.

Moreover, the increasing use of smart contracts, blockchain-based authentication, and algorithmic contracting raises interpretative questions regarding the application of the IT Act. While the statute is technologically neutral, its principles of electronic recognition and authentication continue to provide legal support for such innovations, pending more specialized legislative intervention.

The Information Technology Act, 2000 plays a foundational role in enabling electronic commerce in India by granting legal validity to electronic records, digital signatures, and online contracts, while simultaneously regulating authentication mechanisms and intermediary conduct. Through judicial interpretation and regulatory evolution, the Act has facilitated the growth of India's digital marketplace while embedding safeguards for trust, security, and accountability. Despite emerging challenges posed by advanced digital technologies, the IT Act remains the principal legal framework underpinning commercial activity in India's digital economy.

INTERNET REGULATION AND SERVICE PROVIDER LIABILITY

The regulation of internet intermediaries in India represents a critical intersection between digital governance, freedom of expression, and corporate accountability. The Information Technology Act, 2000 (IT Act), together with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, establishes the legal framework governing the responsibilities, immunities, and compliance obligations of entities that facilitate online communication and content distribution.

A. Definition and Scope of Intermediaries

Section 2(1)(w) of the IT Act defines an "intermediary" broadly to include any person or entity that receives, stores, or transmits electronic records on behalf of another, including internet service providers (ISPs), social media platforms, web hosts, search engines, and cloud service providers.[36]This inclusive definition reflects the legislature's recognition that digital platforms perform diverse functions from passive storage to active transmission and that liability cannot be uniform across actors without consideration of their operational role.

[34] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

[35] Information Technology Act, No. 21 of 2000, § 43A (India).

[36] Information Technology Act, No. 21 of 2000, § 2(1)(w) (India).

B. Conditional Immunity under Section 79

Section 79 of the IT Act provides conditional immunity (safe harbor protection) to intermediaries, shielding them from liability for third-party content hosted, transmitted, or stored on their platforms, subject to the fulfillment of two critical conditions:

i. The intermediary does not initiate the content, modify it, or select recipients; and
ii. The intermediary observes due diligence, including prompt removal of unlawful information upon receiving actual knowledge through a judicial or government order.[37]

This framework is intended to balance innovation and freedom of expression with the need for accountability, enabling digital platforms to operate without constant risk of litigation while ensuring responsiveness to illegal or harmful content.

C. Loss of Immunity and Due Diligence Obligations

Immunity under Section 79 is conditional and revocable. Intermediaries may lose protection if they fail to exercise due diligence, neglect regulatory compliance, or ignore takedown obligations prescribed in the IT Rules.[38] The 2021 Intermediary Guidelines expanded operational obligations, requiring platforms to:

a) Establish grievance redressal mechanisms;
b) Remove or disable access to unlawful content within specific timeframes;
c) Appoint compliance officers and local representatives; and
d) Follow transparency norms for content moderation and algorithmic decision-making.

Non-compliance can trigger legal action under Sections 66A (pre-amendment provisions for illegal content), 66C/66D (identity fraud), and other cybercrime provisions, as well as civil liability for third-party claims.

D. Judicial Interpretation

The Supreme Court in Shreya Singhal v. Union of India (2015) provided the constitutional calibration of intermediary liability.[39] While the Court struck down the overly broad Section 66A for infringing Article 19(1)(a) (freedom of speech), it also read down Section 79 and the associated rules, confirming that intermediaries are obliged to act only upon "actual knowledge" or receipt of a court/governmental order, and cannot be held liable for user-generated content proactively.

The Court emphasized that safe harbor provisions must not be interpreted to impose disproportionate burdens that could stifle online expression or innovation. This judicial interpretation has become a touchstone for platform governance and regulatory compliance in India, balancing constitutional rights with the state's interest in combating cybercrime and unlawful content dissemination.

[37] Id. § 79.

[38] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 149(E) (India).

[39] *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

E. Contemporary Implications for Digital Platforms

In the current Indian digital ecosystem, Section 79 and the Intermediary Guidelines serve multiple commercial and regulatory functions:

Risk Management for Platforms

Conditional immunity enables large social media companies, e-commerce marketplaces, and cloud service providers to operate without continuous litigation exposure for user-generated content.

Enforcement of Digital Accountability

Timely removal of illegal content, transparency reporting, and grievance redressal mechanisms ensure that platforms contribute to lawful digital conduct.

Integration with Cybersecurity and Data Protection

Platforms must align intermediary obligations with Sections 43A and 72A (reasonable security practices and privacy safeguards) as well as emerging frameworks under the Digital Personal Data Protection Act, 2023, ensuring secure and accountable processing of user information.

Through this combination of statutory safe harbor, procedural due diligence, and judicial oversight, India's intermediary liability regime represents a nuanced approach to regulating digital speech, platform accountability, and internet governance.

INTELLECTUAL PROPERTY ASPECTS OF INFORMATION TECHNOLOGY

While the Information Technology Act, 2000 (IT Act) primarily governs electronic transactions, cybersecurity, and cybercrime, it intersects with intellectual property (IP) enforcement in the digital realm.[40] The Act does not create or confer IP rights; rather, claims related to copyright, trademark, or patent infringement must be pursued under the relevant statutes, including the Copyright Act, 1957 and the Trade Marks Act, 1999.[41] Nevertheless, the IT Act facilitates the enforcement of IP rights online, particularly by addressing unauthorized access, digital copying, and distribution of protected content.

A. Interface between IT Act and IP Enforcement

Sections 43 and 66 of the IT Act, which criminalize unauthorized access, data theft, and hacking, are frequently invoked in cases of digital piracy or software infringement.[42] For instance, the illegal downloading or distribution of copyrighted content over peer-to-peer networks can be addressed under Section 43 for civil liability and Section 66 for criminal penalties, in addition to traditional remedies under the Copyright Act.

Courts have reinforced this integrated approach. In Super Cassettes Industries Ltd. v. Myspace Inc., the Delhi High Court recognized that online intermediaries hosting infringing content may face liability under both copyright law and IT Act provisions if they fail to take reasonable measures to prevent

[40] See generally Information Technology Act, No. 21 of 2000 (India).

[41] Copyright Act, No. 14 of 1957, § 51 (India); Trade Marks Act, No. 47 of 1999, § 28 (India).

[42] Information Technology Act, No. 21 of 2000, §§ 43, 66 (India).

unauthorized use.[43] Similarly, in Yahoo! Inc. v. Akash Arora, the court considered the digital context for trademark infringement, highlighting that intermediary platforms may have obligations to remove infringing content, intersecting with IT Act safe harbor rules.[44]

B. Challenges of Digital IP Enforcement

Despite these synergies, the IT Act does not provide explicit "internet IP" provisions, leaving gaps in digital IP enforcement. These gaps include:

1. Limited statutory clarity on intermediary obligations regarding IP-infringing content, beyond Section 79 safe harbor conditions;
2. Absence of express procedural mechanisms for online IP takedown, notification, and counter-notification; and
3. Difficulty in addressing cross-border infringement, given the extraterritorial reach of digital networks and varying international IP standards.

Scholars note that this legislative lacuna has necessitated judicial innovation, with courts effectively using IT Act provisions to complement IP statutes for digital enforcement.[45] This has been particularly evident in software piracy, unauthorized streaming, and social media IP infringement cases.

C. Emerging Mechanisms and Technological Considerations

Recent developments in digital technology, including streaming services, cloud storage, blockchain authentication, and AI-generated content, have further complicated IP enforcement. While the IT Act provides tools to address unauthorized access or hacking of protected works, enforcement of exclusive rights (reproduction, distribution, or performance) remains dependent on IP statutes.

To bridge this gap, the Copyright (Amendment) Act, 2012 introduced provisions allowing intermediaries to be liable for infringing content if they fail to act on notices, harmonizing with IT Act Section 79 due diligence obligations. Similarly, AI-based monitoring systems deployed by e-commerce and content platforms now rely on the IT Act for procedural compliance while using IP law to substantively remove infringing material.

D. Judicial and Scholarly Assessment

Legal scholars observe that while the IT Act supports enforcement infrastructure through provisions on unauthorized access, cybercrime, and intermediary liability it cannot substitute for substantive IP rights.[46] Courts continue to interpret the IT Act flexibly to support IP protection, for instance, recognizing that data exfiltration involving copyrighted material constitutes both a cyber offence and an

[43] *Super Cassettes Industries Ltd. v. Myspace Inc.*, CS (COMM) 144/2008 (Delhi High Court).

[44] *Yahoo! Inc. v. Akash Arora*, 1999 PTC 66 (Delhi High Court).

[45] Pratyush Nath & R. Srinivasan, *Intellectual Property Enforcement in Indian Cyberspace*, 12 J. Indian L. & Tech. 45 (2020).

[46] ibid

IP violation.[47] This integrated approach underscores the evolving nature of digital IP enforcement in India, combining statutory, judicial, and technological instruments.

Thus, IT Act plays a supportive but crucial role in the enforcement of intellectual property online. By criminalizing unauthorized access, hacking, and data theft, and by providing a framework for intermediary responsibility, the Act complements existing IP legislation. However, the absence of explicit internet IP provisions highlights the need for continued judicial interpretation, legislative updates, and technological measures to protect rights in an increasingly digital and globalized environment.

IT AND DOMAIN NAME DISPUTES ADJUDICATION

While the Information Technology Act, 2000 (IT Act) provides a framework for electronic transactions, cybercrime, and intermediary regulation, it is silent on domain name disputes such as cybersquatting, typosquatting, or registrations that are confusingly similar to existing trademarks.[48] Consequently, Indian courts and regulatory authorities have relied on trademark law, common law principles, and specialized domain dispute resolution mechanisms to protect intellectual property in the digital naming space.

A. Judicial Recognition of Domain Names as Trademarks

Indian jurisprudence treats domain names as functional identifiers akin to trademarks, given their role in denoting the source of online goods and services. In Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd., the Supreme Court held that a domain name can attract protection under the Trade Marks Act, 1999 and the common law action of passing off, particularly where it is used in a manner that creates consumer confusion regarding the origin of online services.[49] The Court emphasized that:

a) Domain names, like trademarks, are identifiers of commercial origin;
b) Unauthorized registration or use of confusingly similar domain names constitutes an infringement or passing off; and
c) Remedies under trademark law, including injunctions and damages, are available for such misuse.

This decision remains a cornerstone for adjudicating domain name disputes in India, bridging gaps left by the IT Act.

B. The .IN Domain Name Dispute Resolution Policy (INDRP)

For .IN country-code top-level domains (ccTLDs), India has implemented the .IN Domain Name Dispute Resolution Policy (INDRP), administered by the National Internet Exchange of India (NIXI).[50] The INDRP provides a mandatory arbitration framework, modeled on the international Uniform Domain-Name Dispute-Resolution Policy (UDRP), to resolve disputes where domain registrations conflict with trademark rights. Key features of the INDRP include:

[47] *Indian Performing Rights Society Ltd. v. Sanjay Dalia*, CS(OS) 15/2010 (Delhi High Court).

[48] Information Technology Act, No. 21 of 2000 (India).

[49] *Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd.*, (2004) 6 S.C.C. 145 (India).

[50] .IN Domain Name Dispute Resolution Policy (INDRP), National Internet Exchange of India (NIXI), https://www.nixi.in/indrp (last visited Feb. 2, 2026).

i. Complainants must hold a registered or common-law trademark.
ii. Registration or use of a domain name that is identical or confusingly similar to a trademark, where the registrant has no legitimate interest, and acts in bad faith.
iii. Disputes are resolved through administrative proceedings under the Arbitration and Conciliation Act, 1996, ensuring enforceable arbitral awards.
iv. Transfer, cancellation, or modification of the disputed domain name.

This mechanism allows for efficient, technology-sensitive adjudication without resorting to lengthy judicial processes.

C. International Norms: UDRP and ICANN

Globally, the Uniform Domain-Name Dispute-Resolution Policy (UDRP) under ICANN provides a parallel mechanism for generic top-level domains (gTLDs) such as .com, .net, and .org.[51] The UDRP similarly resolves disputes arising from domain registrations that infringe trademark rights or are used in bad faith. Indian companies operating globally often invoke UDRP procedures for cross-border domain conflicts, while domestic ccTLD disputes are resolved under INDRP.

D. Complementarity with IT Act and IP Enforcement

Although the IT Act does not expressly regulate domain name disputes, its provisions particularly Sections 43, 66, and 79—may intersect with domain disputes in cases involving:

a) Cyber-squatting with unauthorized access to computer systems (Section 43);
b) Hacking of registrar databases (Section 66); and
c) Intermediary responsibilities of domain registrars and hosting providers (Section 79).

This interplay underscores the broader principle that while domain-specific regulations (INDRP/UDRP) provide procedural remedies, statutory IT Act provisions support enforcement and safeguard systemic integrity.

Domain name disputes in India are adjudicated through a combination of trademark law, common law doctrines, administrative arbitration (INDRP), and international frameworks (UDRP). While the IT Act does not directly govern these conflicts, its provisions support enforcement against cyber-enabled misappropriation and ensure that intermediaries, such as registrars and hosting platforms, observe due diligence. Indian jurisprudence, led by Satyam Infoway, has firmly established that domain names carry commercial significance equivalent to trademarks, thereby integrating digital identifiers within the ambit of IP protection in cyberspace.

SEMICONDUCTOR TECHNOLOGY PROTECTION

The Information Technology Act, 2000 (IT Act) does not provide specific protections for semiconductor technologies, such as chip design, fabrication processes, or hardware schematics.[52] The primary statutory protection for semiconductor-related intellectual property in India arises under the Patents Act, 1970,

[51] Uniform Domain-Name Dispute-Resolution Policy (UDRP), ICANN, https://www.icann.org/resources/pages/policy-2012-02-25-en
(last visited Feb. 2, 2026).
[52] Information Technology Act, No. 21 of 2000 (India).

which covers inventions including circuit layouts, fabrication methods, and novel semiconductor devices, and under trade secret law, which protects confidential technical information not publicly disclosed.[53]

A. Intersection of IT Act with Semiconductor IP

Although the IT Act does not create substantive rights over semiconductor technologies, it indirectly safeguards these assets by criminalizing unauthorized digital access and misappropriation. Key provisions include:

Section 43 – Civil liability for unauthorized access

This provision addresses unauthorized copying, transmission, or damage to electronic data, including proprietary semiconductor designs stored digitally.[54]

Section 66 Criminal liability for hacking: Applies to deliberate intrusion into computer systems containing semiconductor-related information, which could constitute industrial espionage or theft of trade secrets.[55]

Section 72A Breach of confidentiality and privacy

Criminalizes the disclosure of sensitive information in breach of lawful contracts, offering protection for chip design schematics or proprietary fabrication data shared electronically under NDAs or licensing agreements.[56]

These provisions collectively enable semiconductor companies to protect digital assets, including design files, software simulations, and CAD schematics, against cyber-enabled misappropriation.

B. Challenges and Emerging Legal Needs

The rapid evolution of semiconductor technologies from AI accelerators to next-generation fabrication nodes has heightened the need for legal clarity regarding IP and trade secret protection in digital contexts. Current challenges include:

i. Cross-border cyber-espionage: Semiconductor designs stored in cloud environments or transmitted internationally are vulnerable to unauthorized access; IT Act extraterritorial provisions (Section 75) provide a partial remedy.[57]
ii. Integration with AI and IoT: Automated design systems and collaborative chip development platforms create new vectors for potential data theft.
iii. Coordination with patent enforcement: While the Patents Act provides substantive rights, enforcing those rights in digital networks requires leveraging IT Act provisions for cybercrime. Policy discussions, including those in the Draft National Semiconductor Policy 2023 and related

[53] Patents Act, No. 39 of 1970, §§ 2, 48–55 (India); see also Trade Secrets Law, common law protections under contract.

[54] Information Technology Act, No. 21 of 2000, § 43 (India).

[55] Id. § 66.

[56] Id. § 72A.

[57] Id. § 75 (extraterritorial application).

technology governance frameworks, recognize the necessity of harmonizing digital law with IP protection for advanced technologies to foster innovation and foreign investment.[58]

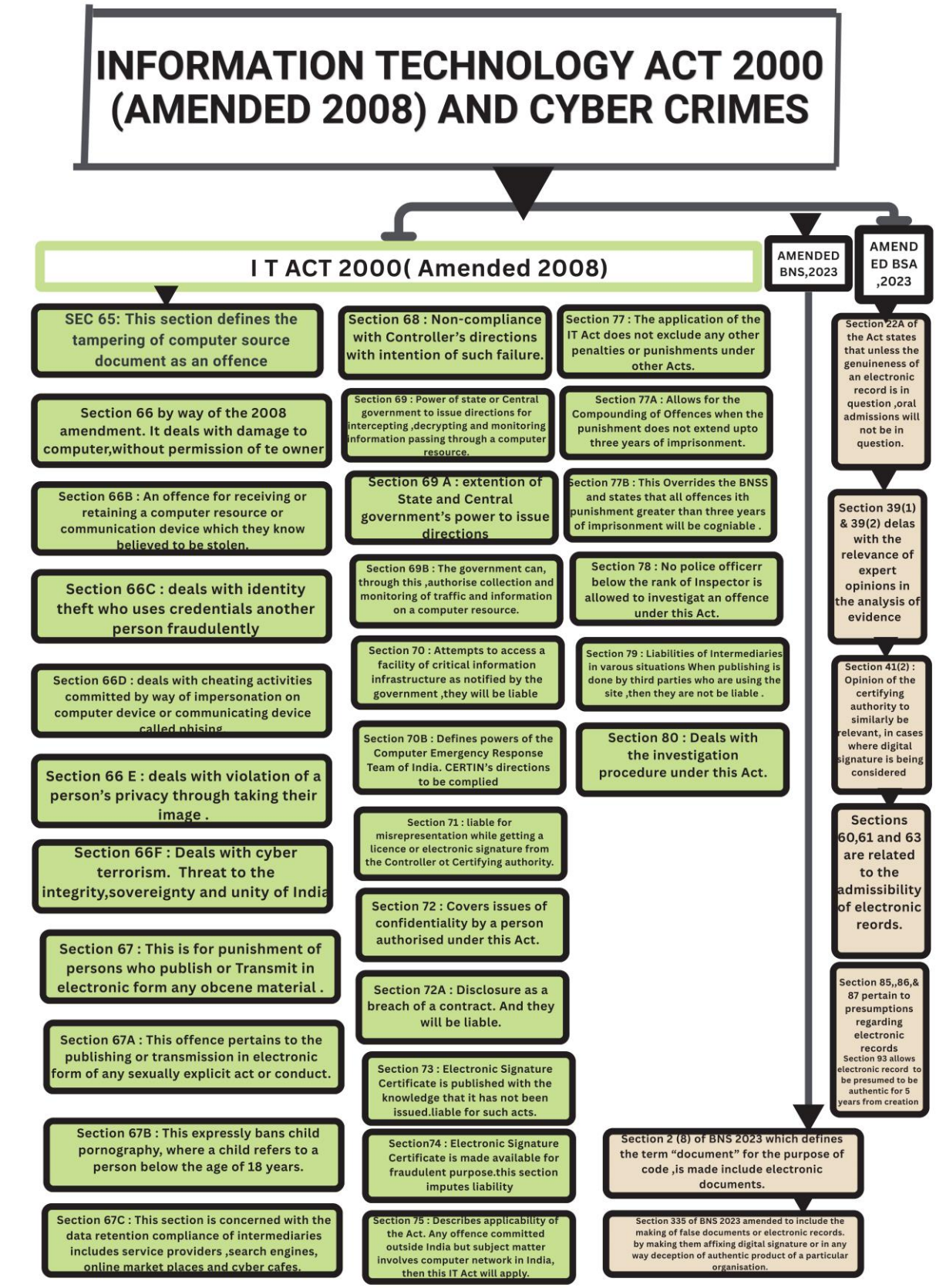
C. Judicial and Scholarly Assessment

Although no reported cases in India specifically involve semiconductor chip designs under IT Act provisions, courts have applied the Act's cybercrime provisions to software piracy, digital schematics, and confidential data breaches, which serve as doctrinal analogues for semiconductor IP protection. Scholars emphasize that Section 43, 66, and 72A are increasingly relied upon in combination with the Patents Act and trade secret law to secure high-value technology assets in the digital ecosystem.[59]

Last but not the least, while the IT Act does not confer direct semiconductor IP rights, it provides complementary legal tools to protect digital representations of semiconductor technologies. Unauthorized access, hacking, and breaches of confidentiality are actionable under the IT Act, and when integrated with patent and trade secret regimes, these provisions form a cohesive framework for safeguarding advanced technology assets in India's digital environment. As semiconductor innovation accelerates, policy and legislative updates may further clarify the interplay between IT law, IP law, and national technology security.

[58] Ministry of Electronics and Information Technology (MeitY), Draft National Semiconductor Policy 2023 (India).

[59] See Pratyush Nath & R. Srinivasan, *Cybersecurity and Emerging Technology IP Enforcement in India*, 15 J. Indian L. & Tech. 78 (2022).


INFORMATION TECHNOLOGY ACT 2000 (AMENDED 2008) AND CYBER CRIMES
I T ACT 2000(Amended 2008)
AMENDED BNS,2023
AMEND ED BSA ,2023
SEC 65: This section defines the tampering of computer source document as an offence
Section 66 by way of the 2008 amendment. It deals with damage to computer,without permission of te owner
Section 66B : An offence for receiving or retaining a computer resource or communication device which they know believed to be stolen.
Section 66C : deals with identity theft who uses credentials another person fraudulently
Section 66D : deals with cheating activities committed by way of impersonation on computer device or communicating device called phising
Section 66 E : deals with violation of a person's privacy through taking their image .
Section 66F : Deals with cyber terrorism. Threat to the integrity,sovereignty and unity of India
Section 67 : This is for punishment of persons who publish or Transmit in electronic form any obcene material .
Section 67A : This offence pertains to the publishing or transmission in electronic form of any sexually explicit act or conduct.
Section 67B : This expressly bans child pornography, where a child refers to a person below the age of 18 years.
Section 67C : This section is concerned with the data retention compliance of intermediaries includes service providers ,search engines, online market places and cyber cafes.
Section 68 : Non-compliance with Controller's directions with intention of such failure.
Section 69 : Power of state or Central government to issue directions for intercepting ,decrypting and monitoring information passing through a computer resource.
Section 69 A : extention of State and Central government's power to issue directions
Section 69B : The government can, through this ,authorise collection and monitoring of traffic and information on a computer resource.
Section 70 : Attempts to access a facility of critical information infrastructure as notified by the government ,they will be liable
Section 70B : Defines powers of the Computer Emergency Response Team of India. CERTIN's directions to be complied
Section 71 : liable for misrepresentation while getting a licence or electronic signature from the Controller ot Certifying authority.
Section 72 : Covers issues of confidentiality by a person authorised under this Act.
Section 72A : Disclosure as a breach of a contract. And they will be liable.
Section 73 : Electronic Signature Certificate is published with the knowledge that it has not been issued.liable for such acts.
Section74 : Electronic Signature Certificate is made available for fraudulent purpose.this section imputes liability
Section 75 : Describes applicability of the Act. Any offence committed outside India but subject matter involves computer network in India, then this IT Act will apply.
Section 77 : The application of the IT Act does not exclude any other penalties or punishments under other Acts.
Section 77A : Allows for the Compounding of Offences when the punishment does not extend upto three years of imprisonment.
Section 77B : This Overrides the BNSS and states that all offences ith punishment greater than three years of imprisonment will be cogniable .
Section 78 : No police officerr below the rank of Inspector is allowed to investigat an offence under this Act.
Section 79 : Liabilities of Intermediaries in varous situations When publishing is done by third parties who are using the site ,then they are not be liable .
Section 80 : Deals with the investigation procedure under this Act.
Section 2 (8) of BNS 2023 which defines the term "document" for the purpose of code ,is made include electronic documents.
Section 335 of BNS 2023 amended to include the making of false documents or electronic records. by making them affixing digital signature or in any way deception of authentic product of a particular organisation.
Section 22A of the Act states that unless the genuineness of an electronic record is in question ,oral admissions will not be in question.
Section 39(1) & 39(2) delas with the relevance of expert opinions in the analysis of evidence
Section 41(2) : Opinion of the certifying authority to similarly be relevant, in cases where digital signature is being considered
Sections 60,61 and 63 are related to the admissibility of electronic reords.
Section 85,,86,& 87 pertain to presumptions regarding electronic records
Section 93 allows electronic record to be presumed to be authentic for 5 years from creation

CONCLUSION

The Information Technology Act, 2000 (IT Act) continues to serve as the cornerstone of India's legal framework for digital governance, encompassing electronic transactions, cybercrime regulation, intermediary liability, e-commerce facilitation, and the digital enforcement of intellectual property rights. By granting statutory recognition to electronic records and digital signatures (Sections 4 and 5), the Act has legitimized online contracting and e-commerce, enabling India's digital economy to expand in both domestic and cross-border contexts. The regulatory framework for Certifying Authorities further reinforces trust in digital authentication mechanisms, ensuring the enforceability and reliability of online transactions.

In the realm of cybercrime and cybersecurity, the IT Act has provided a comprehensive set of civil and criminal remedies. Provisions such as Sections 43, 66, 66C, 66F, and 72A address unauthorized access, hacking, identity theft, cyber terrorism, and breaches of confidentiality, while institutional mechanisms like CERT-In and the National Critical Information Infrastructure Protection Centre (NCIIPC) facilitate proactive incident response and protection of critical digital infrastructure. Judicial interpretations, particularly in Shreya Singhal v. Union of India, have tempered enforcement powers with constitutional safeguards, notably the right to freedom of speech and informational privacy, thereby establishing a balance between state security imperatives and individual liberties.

The IT Act also interfaces with intermediary liability and online platform governance through Section 79 and the Intermediary Guidelines, establishing conditional safe harbor protections that incentivize due diligence while holding platforms accountable for unlawful content. This has been critical in ensuring operational certainty for ISPs, social media platforms, and e-commerce intermediaries while maintaining compliance with constitutional principles and public interest objectives.

In the domain of intellectual property and digital rights, the Act functions primarily as an enforcement adjunct. While it does not create substantive IP rights, it supports protection against cyber-enabled infringement through its provisions on unauthorized access, hacking, and breaches of confidentiality, complementing the Copyright Act, 1957, Trade Marks Act, 1999, and patent and trade secret regimes. Judicial recognition of domain names as functional trademarks in Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd. and the development of the INDRP framework underscore the evolving intersection between IP law, digital commerce, and internet governance.

Emerging technology sectors, including semiconductor design, AI-driven platforms, cloud computing, and IoT ecosystems, highlight the Act's regulatory adaptability and its current limitations. While Sections 43, 66, and 72A provide indirect safeguards for proprietary semiconductor IP and advanced digital assets, the absence of specific provisions for these high-tech domains demonstrates a legislative gap that policymakers and scholars have increasingly noted. Similarly, domain name disputes, cross-border cybercrime, and AI-mediated content governance demand ongoing integration of IT Act principles with specialized legislation and international norms.

In a nutshell, the IT Act represents a foundational yet evolving statute, whose success lies in providing legal certainty for digital transactions, cybersecurity, and e-commerce, while accommodating judicial interpretation and complementary regulatory developments. However, the rapid pace of technological

change spanning AI, semiconductors, and complex platform ecosystems necessitates continuous legislative updates, harmonization with IP and data protection laws, and proactive judicial engagement. Strengthening these intersections will ensure that India's digital legal architecture remains robust, technologically adaptive, and aligned with both global best practices and constitutional safeguards, thereby sustaining trust, innovation, and commercial growth in the digital era.