THE REDWOOD JOURNAL

Website: www.the redwood journal.com

VOLUME:-5 ISSUE NO:-5 , SEPTEMBER 2, 2026

ISSN (ONLINE):- 3139-7360

Email: theredwoodjournal@gmail.com

Digital Number : 2025-23534643

CC BY-NC-SA

Authored By:- Sneha Mishra

THE INFORMATION TECHNOLOGY ACT, 2000: EVOLUTION, CHALLENGES AND CONTEMPORARY RELEVANCE

Abstract

The Information Technology Act, 2000 was India's first comprehensive attempt to give the law a place in electronic commerce and digital communication. It gave legal recognition to electronic records and digital signatures and, at the same time, created a set of computer-related offences. This article traces how the Act developed, starting from its roots in the UNCITRAL Model Law on Electronic Commerce and moving through the major amendment of 2008, which brought in provisions on cyber terrorism, the protection of sensitive personal data and the liability of intermediaries. The study is doctrinal. It reads the statutory text, the leading judicial decisions and the institutions set up under the Act, and it places them alongside the position in other jurisdictions. The main finding is that the Act still provides the legal base for India's digital economy, but it has been slow to respond to artificial intelligence, crypto-assets, cloud computing and cross-border cybercrime, and that its relationship with the Digital Personal Data Protection Act, 2023 remains unsettled during the transition. The article ends with suggestions for reform, among them a clear handover of data protection to the new statute without losing the remedies the old one offered, statutory (rather than only rule-based) provisions for AI-related harms, and regular legislative review.

Keywords: Information Technology Act 2000, cyber law, digital signature, intermediary liability, cybercrime.

1. Introduction

When Parliament passed the Information Technology Act, 2000, the internet was only beginning to change how Indians bought, sold and communicated. The Act had two main aims. The first was to make electronic transactions and digital signatures legally valid so that online commerce could grow with some certainty. The second was to provide a legal framework for punishing offences committed through computers and networks. Before 2000, Indian law had no way of recognising an electronic contract, an electronic record or a digital signature. Businesses that wanted to deal online could not be sure their agreements would hold, and computer misuse fell into a gap that existing criminal law had never been written to cover.

The Act follows the UNCITRAL Model Law on Electronic Commerce, 1996, which the UN General Assembly commended to member states when they made or revised their own laws.[1] The statute has been amended since, most importantly by the Information Technology (Amendment) Act, 2008. That amendment answered a growing list of problems, including cyber terrorism, identity theft and data breaches, and it set out the intermediary liability rules that still shape how online platforms are regulated in India.

The subject deserves attention now because the Act is still central to digital governance even though newer laws have been layered over it. The Digital Personal Data Protection Act, 2023 is the clearest example. It covers ground that the IT Act touched only partly, and the two statutes will sit side by side until the transition is complete. This study has four objectives: to trace the legislative history of the Act; to examine its main provisions on electronic records, digital signatures, cybercrime and intermediary liability; to analyse how the courts have read them; and to ask whether the Act remains adequate for present-day technology. In doing so it asks how the Act has adapted, what gaps are left, and how India's approach compares with that of other countries. The method is doctrinal, relying on statutory text, case law and secondary legal writing. It does not attempt an empirical assessment of how the Act is enforced.

[1]UNCITRAL Model Law on Electronic Commerce 1996, adopted by UN General Assembly Resolution 51/162 (16 December 1996).

2. Evolution of the Act

By the late 1990s the Government of India had accepted that growing electronic commerce needed a legal framework if businesses and consumers were to have any certainty. The Act was passed in 2000 and borrowed heavily from the UNCITRAL Model Law. Its first version was mostly about enabling transactions: it recognised electronic records and digital signatures and created the office of the Controller of Certifying Authorities to oversee digital signature certificates. A few offences, such as hacking and unauthorised access, were included, but over the next decade it became clear that these were too thin to deal with the many forms cybercrime was taking.

The weakness was exposed most sharply in the Bazee.com episode, which showed how little the original Act said about an intermediary's responsibility for content posted by others.[2] That case, together with the report of an expert committee set up by the Ministry of Communications and Information Technology, led to the Information Technology (Amendment) Act, 2008, which came into force in 2009. The amendment widened the Act considerably. It added Section 66A on offensive messages sent through communication services, Section 66F on cyber terrorism, and Section 43A on the duty of body corporates to protect sensitive personal data. It also replaced the earlier provisions on interception and decryption with a wider Section 69, and it recast Section 79 into a conditional safe harbour for intermediaries who observe due diligence. With these changes the Act stopped being mainly a statute for facilitating commerce and became a broader cyber law. Its shape has kept changing since, most notably when Section 66A was struck down in 2015.

3. The Indian Legal Framework

The Act is built around a few main parts. Chapter II provides for the authentication of electronic records through digital and electronic signatures. Chapter III then lays down the principle of legal recognition: where any law requires information to be in writing or in a particular form, that requirement is met if the information is in electronic form and can be accessed for later reference.[3] Computer-related wrongs are dealt with in two places. Section 43, in Chapter IX, imposes civil liability for acts such as unauthorised access, data theft, introducing viruses and denial of service. Chapter XI contains the criminal offences, including Section 66 and, for identity theft and cheating by personation using a computer

[2] *Avnish Bajaj v State (NCT of Delhi)* (2008) 150 DLT 769.

[3] Information Technology Act 2000, s 4 (Chapter III, Electronic Governance). Chapter II (ss 3 and 3A) deals with the authentication of electronic records by digital and electronic signatures.

resource, Sections 66C and 66D. Section 67 punishes publishing or transmitting obscene material in electronic form, and Section 67B carries heavier punishment where the material involves children.

Section 43A requires a body corporate that holds or handles sensitive personal data to maintain reasonable security practices. If it fails to do so and causes wrongful loss, it must compensate the person affected. The detail was supplied by the 2011 Rules made under the Act.[4] Section 69 allows the Central and State Governments to direct the interception, monitoring or decryption of information in the interest of the sovereignty and integrity of India, defence, State security and public order. The procedure and safeguards are set out in the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009. Section 79 gives intermediaries conditional protection from liability for third-party content, provided they comply with due diligence requirements, which are now spelt out in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

The data protection position is in transition. The Digital Personal Data Protection Act, 2023 provides for the omission of Section 43A, and with it the 2011 Rules, but that part of the new Act has been scheduled to take effect only in May 2027.[5] Until then both regimes remain on the books, which leaves some doubt about which one governs a particular breach of sensitive personal data.

4. The International Framework

The Act was drafted with the UNCITRAL Model Law in view. That instrument aimed to remove legal obstacles to electronic commerce and to give electronic records a uniform standing across jurisdictions.[6] On the criminal side, the most comprehensive international instrument is the Council of Europe's Convention on Cybercrime, the Budapest Convention. It sets common definitions for offences such as illegal access, data interference and computer-related fraud, and it makes cooperation in investigation and prosecution easier. India has not joined it, and has pointed to sovereignty concerns about cross-border access to data.

---

[4]Information Technology Act 2000, s 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[5]Digital Personal Data Protection Act 2023, s 44(2). The Act and the Digital Personal Data Protection Rules 2025 were brought into force in phases from November 2025; the provisions amending the Information Technology Act 2000, including the omission of s 43A, are scheduled to take effect in May 2027.

[6]UNCITRAL Model Law on Electronic Commerce 1996, art 5.

On intermediary liability, the European Union's e-Commerce Directive and now its Digital Services Act take a graduated approach. They treat mere conduits, hosting providers and online platforms differently and attach different duties to each. This offers a useful point of comparison for the way Section 79 and the 2021 Rules are developing in India. The General Data Protection Regulation has also influenced Indian thinking on breach notification and security safeguards, and its influence can be seen in the Digital Personal Data Protection Act, 2023, which in several respects replaces the data protection provisions that grew up under the IT Act.

5. Judicial Approach

The most important judicial ruling on the Act is *Shreya Singhal v Union of India*, in which the Supreme Court struck down Section 66A as unconstitutional.[7] The section penalised sending information that was grossly offensive or menacing, or that caused annoyance or inconvenience, through a computer resource. Its vague and wide wording had led to arrests over ordinary social media posts. The Court held that the provision had no reasonable connection with any of the grounds listed in Article 19(2), and that its chilling effect on speech made it void for vagueness and overbreadth. The principle that comes out of the case is that restrictions on free speech must be narrowly drawn, even online, and cannot depend on subjective standards such as annoyance. In the same judgment the Court upheld the blocking power under Section 69A and read down Section 79(3)(b) so that an intermediary is obliged to remove content only after receiving actual knowledge through a court order or a government notification. The decision remains the most cited authority on the limits of regulating speech in cyberspace.

Electronic evidence has been the other main area of litigation. In *Shafhi Mohammad v State of Himachal Pradesh*, the Supreme Court held that the certificate required by Section 65B(4) of the Indian Evidence Act, 1872 could be dispensed with where the person producing the record did not control the device it came from.[8] A three-judge bench overruled this in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, holding that the certificate is mandatory for admitting electronic records as secondary evidence, subject to narrow exceptions.[9] Readers should also note that the Indian Evidence Act has since been replaced by the

---

[7] *Shreya Singhal v Union of India* (2015) 5 SCC 1.

[8] *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801.

[9] *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

Bharatiya Sakshya Adhiniyam, 2023, and Section 65B has given way to Section 63, which keeps the certificate requirement and adds details such as a hash value.[10]

Taken together, these decisions show the courts doing two jobs. They have limited the misuse of the Act's penal provisions, and they have settled what follows in evidence from the Act's recognition of electronic records. They also show how much the practical working of a statute that has seen little amendment depends on judicial interpretation.

6. Comparative Analysis

Many other jurisdictions have gone for more specialised laws that are updated more often. In the United States, cybercrime is handled mainly under the Computer Fraud and Abuse Act, 1986, along with sector-specific statutes and state breach-notification laws. The result is a patchwork, but one that keeps changing. The United Kingdom's Computer Misuse Act, 1990 is older than the Indian Act, yet it has been amended from time to time to cover offences such as denial-of-service attacks and supplying tools for computer misuse. It works alongside the Data Protection Act, 2018 and separate online safety legislation. Canada relies on provisions of its Criminal Code and on the Personal Information Protection and Electronic Documents Act. Australia introduced computer offences into its Criminal Code through the Cybercrime Act, 2001, and has a separate Privacy Act, 1988. Singapore, like India, has tried to keep its cyber offences in one place through the Computer Misuse Act, 1993 and the Cybersecurity Act, 2018, but it has updated them more often in response to threats such as ransomware and attacks on critical infrastructure.

India, by comparison, still depends on a single statute that is more than twenty-five years old and was last substantially amended in 2008. Its newer regulation has come mostly through delegated legislation rather than amendments to the Act itself. The gap is most visible in artificial intelligence, cloud computing and offences involving crypto-assets.

7. Challenges and Issues

Several problems limit how well the Act works today. The first concerns artificial intelligence. The Act has no provisions on AI, machine learning or algorithmic decision-making, so harms such as deepfake-enabled fraud and impersonation have to be fitted into general provisions like Sections 66C and 66D, which were never written with such technology in mind. The government has responded through delegated legislation: the 2026

[10]Bharatiya Sakshya Adhiniyam 2023, s 63, in force from 1 July 2024.

amendment to the Intermediary Rules brought "synthetically generated information" within the due diligence framework, with labelling and faster takedown duties for platforms.[11] This is a useful step, but it binds intermediaries rather than the people who create deepfakes, it is mainly concerned with audio and visual content, and it rests on rule-making power instead of a clear statutory provision.

The second problem is the overlap with the Digital Personal Data Protection Act, 2023. Until Section 43A and the 2011 Rules are omitted, two sets of rules coexist, and it is not always clear which applies to a given breach. There is also a concern about what will be lost. Section 43A gave an affected person a right to compensation, and commentators have pointed out that the new Act is built mainly around penalties and does not provide an equivalent remedy to the individual.

The third problem is surveillance. Section 69 and its Rules were framed before the Supreme Court's decision in *Puttaswamy*, which recognised privacy as a fundamental right and set out a proportionality test for state intrusion.[12] The interception framework has not been thoroughly revisited in light of that test, and it still lacks independent oversight. Fourth, the Act has no provisions specific to cryptocurrency or blockchain-based transactions. Offences such as exchange hacks, ransomware payments and fraud have to be prosecuted under the general provisions. Finally, cross-border cybercrime is hard to enforce. Section 75 gives the Act extraterritorial reach, but it has seldom been used in practice, because India lacks strong mutual legal assistance arrangements for cybercrime and has stayed outside the Budapest Convention.

8. Suggestions and Recommendations

Based on these problems, a few recommendations follow. First, the handover from the IT Act to the Digital Personal Data Protection Act should be managed carefully. Parliament and the government should make clear which regime applies in the transition period, and should consider whether the compensation remedy that Section 43A offered needs to be kept in some form. Second, harms from artificial intelligence and deepfakes should be addressed in the statute itself, perhaps through a dedicated chapter, and not only through rules. The European Union's Artificial Intelligence Act is one model that could be studied.

---

[11] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, notified on 10 February 2026 and in force from 20 February 2026.

[12] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

Third, the interception framework under Section 69 should be reviewed so that it meets the proportionality standard in *Puttaswamy*, including independent oversight of interception orders. Fourth, India should rethink its position on international cooperation against cybercrime. It could join a suitable international convention, or it could negotiate bilateral mutual legal assistance treaties designed for cybercrime investigations. Fifth, cyber law statutes should carry built-in review mechanisms, such as sunset or mandatory review clauses, so that the law is updated regularly and not only after problems have already arisen.

9. Conclusion

The Information Technology Act, 2000 has been central to India's digital legal framework. It gave legal standing to electronic transactions and laid the first foundation for dealing with cybercrime. The 2008 amendment was a needed response to more complex threats, and later court decisions, especially *Shreya Singhal*, brought the penal provisions into line with constitutional guarantees of free speech. Even so, the Act is increasingly tested by developments its drafters could not foresee, including artificial intelligence, crypto-assets and large-scale data processing, and by the arrival of a new data protection statute. If it is to stay a coherent and effective instrument of digital governance, it needs a comprehensive review that settles the overlap with data protection law, deals with new technological harms in the statute itself, and strengthens the safeguards around surveillance.

10. References

- The Constitution of India, 1950.
- The Information Technology Act, 2000.
- The Information Technology (Amendment) Act, 2008.
- The Digital Personal Data Protection Act, 2023.
- The Digital Personal Data Protection Rules, 2025.
- The Indian Evidence Act, 1872.
- The Bharatiya Sakshya Adhiniyam, 2023.
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- Radha Ranjan and Pallavi Singh, "Cyber Crime Against Women in Cyber Space: A Critical Analysis of Indian Legislations," 10(1A) Kanpur Philosophers (2023).

- Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.
- Radha Ranjan et al., 'Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches' in Policies Against Fraud and Cybercrime: Strategic, Legal, and Technological Approaches 217–263 (IGI Global Scientific Publishing, 2026), DOI: 10.4018/979-8-3373-5992-2.ch007.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2026.
- UNCITRAL Model Law on Electronic Commerce, 1996.
- Council of Europe, Convention on Cybercrime (Budapest Convention), 2001.
- General Data Protection Regulation (EU) 2016/679.
- *Shreya Singhal v Union of India* (2015) 5 SCC 1.
- *Avnish Bajaj v State (NCT of Delhi)* (2008) 150 DLT 769.
- *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801.
- *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.
- *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.
- Duggal P, *Cyber Law: The Indian Perspective* (Universal Law Publishing).
- Ministry of Communications and Information Technology, Government of India, *Report of the Expert Committee on Amendments to the Information Technology Act, 2000*.
- Ministry of Electronics and Information Technology, Government of India, available at https://www.meity.gov.in.
- Radha Ranjan, Bheem Singh Meena and Shyam Kumar Anand, "Virtual Meetings Under Attack: Assessing the Legal and Security Risks of Zoom Bombing in the Digital Era," 4(2) ShodhKosh: Journal of Visual and Performing Arts (2023).
- Radha Ranjan and Jivantika Gulati, "The Sexual Harassment against Women in Cyber Space: Concept, Reality and the Law," 10(1) Kashmir Journal of Legal Studies 79–90 (2023).