Delhi Metropolitan Education
Affiliated to GGSIP University, New Delhi & Approved by Bar Council of India

RESEARCH ARTICLE
doi: 10.53361/dmejl.v6i01.03

The Evolution of India's Cyber Law: A Legislative Analysis of The Information Technology Act, 2000 and its Amendments

Aditya Singh*

LL.M (Innovation, Technology and Intellectual Property Laws), Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR), Symbiosis Law School, Pune, Symbiosis International (Deemed) University, Pune-411014, Maharashtra, India.

ARTICLE INFO

***Correspondence:**
ars.aditya1@gmail.com
LL.M (Innovation, Technology and Intellectual Property Laws), Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR), Symbiosis Law School, Pune, Symbiosis International (Deemed) University, Pune-411014, Maharashtra, India.

Dates:
Received: 18-04-2025
Accepted: 19-05-2025
Published: 30-06-2025

Keywords:
Cybersecurity, Electronic Transactions, Digital Signatures, IT Act 2000, Data Protection, Intermediary Liability

How to Cite:
Singh, A. (2025) The Evolution of India's Cyber Law: A Legislative Analysis of The Information Technology Act, 2000 and its Amendments. DME Journal of Law, 6(1), 17-26. doi: 10.53361/dmejl.v6i01.03

DME
Journal of Law

Abstract

The Information Technology (IT) Act, 2000, India's first cyberlaw that lays the foundation of the nation's digital legal system, is examined in this legislative study together with its origins, goals, clauses, modifications, and criticisms. Rooted in the UNCITRAL Model Law, the Act was a first step in giving legal validity to electronic transactions and digital authentication in India and was adopted to handle the developing issues of electronic commerce, digital signatures, and cybercrime. By means of a thorough analysis of its legislative history and significant amendments, most notably the IT Amendment Act, 2008, and later laws in 2018 and 2021. This legislative analysis assesses how the Act changed to address new-age cyber dangers and growing privacy issues. The analysis also includes historic court rulings that profoundly affected its interpretation and execution; Shreya Singhal v. Union of India and Justice K.S. Puttaswamy v. Union of India.

Although the IT Act set the foundation for e-governance, intermediary control, and cybersecurity, it has come under fire for jurisdictional uncertainty, poor protection of intellectual property rights, and scant coverage of developing cybercrimes. The IT Act is compared with the proposed Digital India Bill, which aims to modernize India's cyberspace by means of structured control for digital platforms, artificial intelligence, and platform accountability, addressing digital platform responsibility. Emphasizing the need for a dynamic legislative framework that constantly adjusts to technological developments, therefore assuring safe digital governance and maintaining constitutional rights in the digital age, the paper ends.

Introduction

Say you are doing an online transaction, moving money across a digital payment system, or signing an important document using an electronic signature. But what if someone intercepts your transaction, changes your information, or fakes your digital signature? Who would you hold accountable? Here, the Information Technology (IT) Act, 2000 is the place. It is a law on electronic transactions, digital signatures, and cybersecurity. It does this in order to protect your personal and financial information online and sets penalties for cybercrimes so that your privacy is respected. As technology is advancing

rapidly and electronic communication is increasing, India felt the need for strong cyber laws. This is because the act is meant to regulate the use of computers, networks, electronic data, and digital fraud and hacking. But as more people started doing their digital transactions, new problems cropped up and had to be tackled, and the law was made stronger. To deal with these problems, the IT Amendment Bill, 2006, was introduced in the Indian Parliament in December 2006 in Lok Sabha as well as in Rajya Sabha. The IT Amendment Act, 2008, was after a thorough review of the Parliamentary Standing Committee on IT and came into force on October 27, 2009.[1] This amendment strengthened the legal recognition of electronic records, digital signatures, and cybersecurity measures and held service providers responsible for protecting the data. Although these improvements have been made, the enforcement of the IT Act has faced certain gaps and challenges, which need to be further refined as technology progresses. While amendments have closed all the loopholes in the law, but still the law needs continuous updates to meet the requirements of the time and demands of the digital economy and the business sector.

Legislative History of The Information Technology Act, 2000:

The Indian Parliament passed the Information Technology (IT) Act, 2000, on October 17, 2000, to address legal challenges related to electronic transactions, cybercrimes, and digital authentication. The Act is based, in the main, on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, 1996, which is based on the recommendation of a UN General Assembly resolution of 30 January 1997. India's legislation on cybercrime and electronic commerce is also significant as it was one of the first 12 countries in the world to have such legislation.

Countries were guided on how to create their own regulations on e-commerce, digital transactions, and cybersecurity by the UNCITRAL Model Law.[2] Therefore, in order to protect the data, to facilitate secure digital transactions, and to recognize the electronic records and digital signatures as legally valid, the IT Act was developed by India. The Act further spells out the intermediary's responsibilities and prescribes penalties for cyber offenses.

The IT Act was amended to keep pace with the technological advancements and emerging cyber threats. With the coming into force of the IT Amendment Act, 2008 w.e.f 27th October, 2009, provisions pertaining to cyber terrorism, data protection, and the obligations of online service providers were added. In 2018, there were further revisions to incorporate measures to strengthen cybersecurity and also address data privacy concerns.[3]

The nature of the offence is that whether it is committed in or outside of the geographical boundaries of India, irrespective of the nationality of the offender, the Act is applicable on all such offences committed anywhere in India. In addition, it gives legal recognition to electronic contracts and to arbitration processes, creating a structured legal framework for settling disputes in the digital space.

The enactment of the IT Act 2000 was to provide a secure digital environment, support e-commerce growth, and protect the national intellectual property (IP) online.

Objective of The it Act, 20000

The Information Technology Act, 2000, was established to set rules for electronic transactions, cybersecurity, and digital governance in India.[4] Here's a breakdown of its goals:

Legal Recognition of Electronic Records

This Act confirms that electronic records are legally valid. It means that digital information can be officially used in business and government matters

1 Yogesh Kolekar, "A Review of Information Technology Act, 2000" (28 May 2015) https://ssrn.com/abstract=2611827 (last visited 28 March 2025).

2 UNCITRAL, *Model Law on Electronic Commerce with Guide to Enactment 1996*, available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (last visited 30 March 2025).

3 Katie Terrell Hanna, "Definition: Information Technology Amendment Act 2008 (IT Act 2008)", *TechTarget*, https://www.techtarget.com/whatis/definition/Information-Technology-Amendment-Act-2008-IT-Act-2008 (last visited 30 March 2025).

4 Nisha Advani, "The Evolution of Indian Cyber Law: Past, Present, and Future" (2015) 14 *Cyber Legal Studies* 55.

under Indian law, making electronic documents more useful.

Legal Recognition of Digital Signatures

Handwritten signatures can be forged or altered, which is a risk in online transactions. The IT Act gives legal validity to digital signatures, providing a safer way to sign documents and agreements online.

Legal Recognition of Electronic Governance (E-Governance)

The legislation promotes the adoption of technology in government through legally authenticating electronic records and dealings. Public services become more efficient, and the public gains faster access to information, services, and education.

Punishment for Cyber Crimes

The Indian Penal Code, 1860, was not able to address cybercrimes in their entirety. The IT Act includes specialized cybercrimes such as hacking, identity theft, and data breach, together with penalties, furthering India's legal response against cybercrime.

Setup of the Cyber Appellate Tribunal

This act establishes a Cyber Appellate Tribunal (CAT) to deal with the appeals in relation to such decisions taken in accordance with its rules. This facilitates more effective resolution of cyber legal issues.

Amending Existing Laws to Comply with Technology

The Law brings many outdated legislations up to date with contemporary technology, e.g.,

1. Indian Penal Code, 1860 – Contains provisions for cybercrimes.
2. Indian Evidence Act, 1872 – Admits electronic records as evidence before a court.
3. Banker's Book Evidence Act, 1891 – Recognizes electronic banking records.
4. Reserve Bank of India Act, 1934 – Favors digital financial transactions.

In short, by implementing these changes, the IT Act, 2000, creates a strong legal framework for online commerce, digital signing, and cybersecurity, ensuring a secure digital environment in India.

Table 1: STRUCTURE OF THE ACT

S.no		
01.	Chapter 1- PRELIMINARY	Section 1-2
02.	Chapter 2- DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE	Section 3-3A
03.	Chapter 3- ELECTRONIC GOVERNANCE	Section 4-10A
04.	Chapter 4- ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS	Section11-13
05.	Chapter 5- SECURE ELECTRONIC RECORDS AND SECURE ELECTRONIC SIGNATURE	Section 14-16
06.	Chapter 6- REGULATION OF CERTIFYING AUTHORITIES	Section 17-34
07.	Chapter 7- ELECTRONIC SIGNATURE CERTIFICATES	Section 35-39
08.	Chapter 8- DUTIES OF SUBSCRIBERS	Section 40-42
09.	Chapter 9- PENALTIES, COMPENSATION AND ADJUDICATION	Section 43-47
10.	Chapter 10- THE APPELLATE TRIBUNAL	Section 48-64
11.	Chapter 11- OFFENCES	Section 65-78
12.	Chapter 12- INTERMEDIARIES NOT TO BE LIABLE IN CERTAIN CASES	Section 79
	Chapter 12A- EXAMINER OF ELECTRONIC EVIDENCE	Section 79A
	Chapter 13- MISCELLANEOUS	Section 80-94
	The First Schedule	
	The Second Schedule	
	The Third Schedule (Omitted)	
	The Fourth Schedule (Omitted)	

Summarizing The Provisions

Applicability (Sec.1)

The IT Act, 2000 applies everywhere in India. It also covers crimes committed outside India if they affect India's digital systems. (extraterritorial applications, but based on certain conditions as mentioned u/s 74 of the act)

Definition clause

Sec. 2 explains important terms like "computer" and "computer network," etc, which help us understand the context in which these terms shall be interpreted when there is any ambiguity.

Digital Signatures and Electronic Records (Sec. 3-10A)

This act gave legal recognition to electronic signatures and digital records, so digital documents and digital signatures are as valid as physical ones. Sec. 3 deals with digital signatures, which must be unique, can be verified, and are secure. Sections 4 and 5 make the electronic records and signatures legally valid, giving the same sanctity as physical documents and handwritten signatures.

Section 10A allows for digital contracts, making online agreements legally enforceable. The section also helps to achieve the objective of the act, that is e-commerce, and helps businesses do transactions online safely.

Electronic Governance (Sections 11-13)

The IT Act supports electronic governance by recognizing digital government transactions as legally valid. Sec. 12 provides rules for accepting electronic records, ensuring that official digital communications can be enforced legally.

Section 13 outlines when and where electronic records are deemed sent and received, used for legal purposes. Such sections ensure government operations become more effective by minimizing the use of paper and facilitating services.

Digital Certificates and Certifying Authorities (Sections 17-39)

For trust in digital transactions, the Act establishes conditions for certifying authorities. Section 17 establishes the Controller of Certifying Authorities (CCA), who is in charge of licensing the issuing of digital signature certificates.

The procedures for issuing, renewal, suspension, and revocation of digital certificates are described in Sections 18 through 34 in order to make the certificates accurate and trustworthy. Authority for issuing electronic signature certificates has been vested in certifying authorities in Section 35, and Section 39 identifies when suspending or revoking such certificates can be done in order to uphold the trustworthiness of digital systems.

Subscribers' Obligations (Sec. 40-42)

Users of digital signatures are under certain obligations to maintain security. Section 40 mandates users to use authentic digital signatures. Section 41 instructs them to maintain control of their private key and, in the occurrence of any breach in security, report it. According to Section 42, subscribers are notified in the event of revocation of their digital signature certificate. This is intended for ensuring digital authentication.

Cyber Appellate Tribunal (Sec. 48-64)

The IT Act sets up the Cyber Appellate Tribunal (CAT) for adjudicating disputes in cybercrimes and online transactions. Section 48 outlines its establishment for dealing with cases involving digital fraud and hacking effectively. Sections 49-64 refer to the powers of the tribunal, for example, summoning witnesses and giving judgments. Section 52 empowers it with the same powers as a civil court. Section 57 declares its judgments conclusive unless challenged in a High Court, giving a specialist forum for hearing cyber law disputes speedily and effectively.

Cyber Offenses and Investigation (Sec. 65-78)

This part of the law explains Table 2 cybercrimes and their penalties-

Extraterritorial Jurisdiction (Sec. 75) This provision covers cybercrimes that are perpetrated outside of India yet involve Indian systems or networks. The IT Act allows for prosecution of the criminal regardless of their place of origin.

Confiscation of Digital Assets Authorities (Sec.76) have the power to seize computers, systems, or digital devices if used in violation of the Act. The accused

Table 2: Cyber Offenses and Investigation (Sec. 65-78)

Section 43 – Penalty for Damages	You are responsible for paying for any damage you cause to another person's computer system or network. This involves gaining unauthorized access to computers, downloading information without authorization, infecting computers with viruses, or stopping services.
Section 44 – Documentation and Reporting	A punishment of up to INR 1,50,000 may be imposed for failing to submit necessary paperwork or reports to the Controller or Certifying Authority. You could be penalized INR 5,000 every day for failing to submit information on time. A fine of INR 10,000 per day is imposed for improper record keeping.
Section 65 – Manipulating Source Documents	If you intentionally change, hide, delete, or alter the source documents on a computer, you could be fined up to INR 2,000,000 or imprisoned for three years. This regulation guarantees the accuracy and reliability of digital records.
Section 66 – Dishonesty and Fraudulence	Computer-related fraud or dishonesty, such as those covered by Section 43, can result in a fine of up to INR 5,00,000 or three years in prison. This covers data fraud, identity theft, and hacking.
Section 66B – Receiving Stolen Computer Resources	Keeping or receiving a stolen computer resource or device can lead to a fine of INR 1,00,000 or three years in jail if done dishonestly or fraudulently.
Section 66C – Identity Theft	Using someone else's electronic signature, password, or ID fraudulently is a crime, with a fine of up to INR 1,00,000 or three years in jail.
Section 66D – Online Impersonation	Pretending to be someone else online to deceive others can result in a fine of up to INR 1,00,000 or three years in jail.
Section 66E – Violation of Privacy	Sharing private pictures of someone without their agreement can lead to a fine of up to INR 2,00,000 or up to three years in jail. This protects personal privacy.
Section 66F – Cyber Terrorism	Threatening India's unity, integrity, or security through online actions is a severe crime, with life imprisonment as punishment.
Section 67 – Publishing or Transmitting Obscene Content	Sharing obscene material online can lead to a fine of up to INR 5,00,000 or three years in jail. Repeating the offense increases the fine to INR 10,00,000 and five years in jail.
Section 67A – Publishing Sexually Explicit Content	Posting such content can result in a fine of up to INR 10,00,000 or five years in jail. A second offense has stricter penalties, including imprisonment of up to seven years.
Section 68 – Powers of the Controller	The Controller can issue orders to Certifying Authorities or their employees. Disobeying these orders can lead to a fine of INR 1,00,000 or up to two years in jail.
Section 69 – Government's Power to Intercept Data	For the sake of national security, the government may have agencies intercept or decrypt communications. Not obeying these orders can result in imprisonment of up to seven years alongside a monetary penalty.
Section 70 – Protected Systems	The government can declare certain computer systems "protected." Unauthorized access to these systems brings ten years in jail and a fine.
Section 71 – Misrepresentation or Suppression of Facts	Providing false information for a license or electronic signature certificate can lead to a fine of INR 1,00,000 or two years in jail.
Section 72 – Breach of Confidentiality and Privacy	Revealing another person's sensitive information without their consent is punishable by a fine of INR 1,00,000 or imprisonment of no more than 2 years. If done maliciously, the punishment increases to a fine of INR 5,00,000 and up to 3 years in prison
Section 73 – Fraudulent Electronic Signature Certificates	An individual found to be publishing or circulating an Electronic Signature Certificate not officially issued or known inaccurate is subject to a penalty not exceeding 1 lakh rupees. In addition, a maximum of two years in prison may be enacted.
Section 74 – Creation of Fraudulent Electronic Certificates	A fine of INR 1,00,000 and a maximum sentence of two years in prison await anyone who wilfully creates, publishes, or distributes phony electronic signature certificates for illicit purposes.

have the opportunity to prove that these items were not used for illegal activities to prevent confiscation.

Section 80 Empowers police officers ranked Inspector or higher to investigate cybercrimes, ensuring law enforcement can handle digital offenses effectively.

Amendments to The Act

Amendment in 2008

Section 66A of the Act was amended in the year 2008. It became controversial as it provided for imprisonment for the misuse of offensive messages through electronic communication. Any message that caused hatred and any message that threatened national security were prohibited. But the government failed to define what "offensive" meant, and the consequence was the arrest of countless people.[5] In the year 2015, the Supreme Court struck down this section in the case of *Shreya Singhal vs. Union of India*.[6]

Amendment Bill 2015

The 2015 amendment bill sought to modernize the law in a way that would more effectively protect the rights of people as enshrined in the Constitution. It also amended Section 66A that pertained to offensive messages on the internet but failed nonetheless to define what messages were considered objectionable.[7] The Supreme Court struck down this section in the case of Shreya Singhal as it contravened Article 19, which ensures free speech.[8]

Information Technology Intermediary Guidelines (Amendment) Rules 2018

In 2018, the government issued regulations to make internet intermediaries accountable. Intermediaries have to revise their privacy policies with the goal of shielding citizens against illegal activities such as pornography, offensive communications, and hate speech. Provide information as needed to the government with the reason for national security, within a time frame of 72 hours each intermediary designate a 'nodal person of contact' who will be present 24/7. Provide for breaking the end-to-end encryption for tracking harmful messages when needed.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

In 2021, regulations for online platforms were rolled out in India. Platforms have the obligation to resolve issues and respond to grievances in two weeks. There are new regulations for news publishers as well, which were criticized as being a curb on freedom of speech and the press. User information must be shared with the government if there's a security risk, but users can still take the matter to court.

Jan Vishwas (Amendment Provisions) Act, 2023

This act seeks to simplify business operations and eliminate criminal charges for minor violations in a series of laws, one being the IT Act, 2000. A primary purpose is to make things easier for businesses and people, ensuring the penalty reflects the nature of the offense. A significant adjustment is that some offenses under the IT Act are now not criminal offenses. Some parts of the Act previously could lead to imprisonment for minor violations. Now, these have been substituted with fines, meaning there is no fear of jail for lesser violations. This adjustment ensures that people and companies don't fear criminal charges for minor procedural errors. This act ushered in fines related to the severity of the offense. This ensures the penalty is fair and corresponds with the nature of the violation.[9]

Landmark cases

Shreya Singhal vs. Union of India[10] (2015)

This legal examination explored the legitimacy of Section 66A within the Information Technology Act,

5 Press Information Bureau, "Release ID 53617", http://pib.nic.in/newsite/erelease.aspx?relid=53617 (last visited 1 April 2025).

6 *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

7 Lok Sabha, *Parliamentary Report on the Information Technology Act*, https://eparlib.nic.in/bitstream/123456789/748215/1/3472.pdf.

8 Columbia Global Freedom of Expression, "*Shreya Singhal v. Union of India*", https://globalfreedomofexpression.columbia.edu/cases/shreya-singhal-v-union-of-india (last visited 1 April 2025).

9 Jaspreet Singh, "What Is 'Overcriminalisation' and How Does the Jan Vishwas (Amendment of Provisions) Bill, 2022 Deal with It?" (2023) 6 *International Journal of Law Management and Humanities* 303.

10 *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

2000. An online offensive message emerged from this law. The Supreme Court ruled the measure unconstitutional because it breached the Indian Constitution's protections for freedom of speech and expression.

Shreya Singhal vs. The 2015 ruling initiated legal proceedings that examined additional sections of the IT Act, 2000, which addressed online content restrictions and platform responsibilities. The Supreme Court examined legal sections to determine their constitutionality which assisted in establishing digital platform regulations in India.

Justice K. S. Putswami vs. Union of India[11] (2017)

This significant ruling established privacy rights as fundamental components of life and personal liberty protections under Article 21. The evolution of data security laws experienced significant advancement while privacy rights gained robust reinforcement during the digital age.

Justice P. N. Varadarajan v. Union of India[12] (2015)

The Supreme Court ruled that the IT Act of 2000 does not provide the government with the authority to intercept and/or monitor electronic communications without constraints. There are legal standards that must be met in order to carry out such actions without being labeled as unauthorized watching.

Criticism of the it Act, 2000

jurisdictional Conflicts

The IT Act, 2000 has issues related to jurisdiction because the internet spans across countries. This makes it challenging to know which laws should be followed and how to enforce them properly when dealing with online activities and disputes.

Lack of Provisions for Domain Name Issues

Business on the internet greatly depends on domain names. But the IT Act, 2000 is devoid of answers to questions such as who can be entitled to domain names, who will be responsible for domain holders, and how disputes regarding domain name registration can be settled. Thus, businesses and people working in the cyberspace remain in a state of uncertainty.

The Act does not have proper Intellectual Property Rights (IPR) protection. Therefore, the Act is ineffective in dealing with matters of copyrights and patents, especially in the case of software, digital content, and intellectual properties based on the internet. This may lead to intellectual properties being used in a way that they should not and be misused and infringed upon by the use of the internet.

Cyber Crime: Limited Scope of Offenses: The law deals with limited number of cybercrimes. The evolution of technology has brought about new cyber crimes such as cyber stalking, identity theft, phishing, online fraud, chat room abuse, hijacking internet time etc. The new dangers of this type are not covered holistically under the law and thus there are loopholes in the protection from such criminal activities.

Privacy protection and content regulation in IT Act, 2000 are lacking. This is a cause of worry because data breach, and online surveillance by unauthorized persons, spread of offensive content, etc. are possible. Such issues have to be resolved for the cyber environment to be secure.

Implementation Challenges

The Act does not explicitly include how it is to be enforced or regulated. The result is that there is no clear guidelines, which leads to difficulties in maintaining consistent compliance. This makes it difficult to ensure the success of the Act to tackle the problems in the digital world.

Analysis with Comparison

Digital India Bill

The overarching framework provided by the IT Act of 2000 which governs online activities in India will be repealed and replaced by the Digital India Bill. The IT Act has over two decades of history and has helped shape the contours of various domains such as digital transactions and cybersecurity, along with

11 *Justice K.S. Puttaswamy v. Union of India*, AIR 2017 SC 4161.
12 *Justice P.N. Varadarajan v. Union of India*, (2015) 13 SCC 472.

obligations of service providers. As with much of legislative policy, it has failed to address emerging technology issues such as AI, blockchain, and digital media. The purpose of the Digital India Bill is to enhance the management of digital issues in India through platform responsibility frameworks, content moderation guidelines, AI regulation, and establishing punitive measures for cyber offenses.

Regulation Scope and Aims

The IT Act, 2000, focused primarily on enabling online commerce, cyberspace security, and digital signatures. It addressed matters such as online deception, hacking, and use by the government of digital instruments, but it did not fully encompass regulation of digital platforms, AI, disinformation, or threats resulting from emerging tech, but the Digital India Bill takes a broader approach. It classifies intermediaries into a risk hierarchy and enforces rules according to each class. This manner of determining risk ensures that digital platforms are regulated according to the extent they are likely to shape the world online, the sensitivity of the data they handle, and the extent they can be harmful online.

In addition, the IT Act, 2000, makes use of a disorganized system for implementing rules via CERT-In (Indian Computer Emergency Response Team) and the law enforcement agencies. The Digital India Bill proposes the creation of a special internet regulating body. This would be the same as other present mechanisms such as the Telecom Regulatory Authority of India (TRAI) or the Securities and Exchange Board of India (SEBI). This regulator arrangement by the DIB would make digital platforms follow harmonious rules and would tackle cybersecurity, content moderation, and AI governance more effectively.[13]

Intermediary Liability and Platform Accountability

The IT Act, 2000 incorporated the "safe harbor" provision in Section 79. It protected the intermediaries against liabilities for content created by other people, provided they complied with government regulations on the removal of specified content. This ensured a singularly important boost to digital growth and averted much legal issues for platforms. This nonetheless created ineffective attempts against cyber problems such as misinformation, cyber fraud, and fake videos, but the Digital India Bill will modify the "safe harbor" rules with varying degrees of responsibility depending on the risk a platform generates.

For example, bigger social media platforms, AI-based search engines, and large e-commerce portals will have more stringent standards in place for content moderation and the curtailment of misinformation in line with government regulations. The Bill mandatorily expects these platforms to take down illegal content proactively, which will be the responsibility of the companies rather than the government agencies. This way, the middlemen become more accountable for the decrease in online harms but not at the cost of promoting free speech and innovation.[14]

Cybercrime and Digital Offenses

The IT Act 2000 made a big leap in addressing the cybercrimes of hacking, identity theft, and online scams. Yet, it falls short of providing for contemporary threats such as videos with AI manipulation, online disinformation, cyberbullying, and fraudulent transactions. The Digital India Bill proposes increasing the offenses subject to legal liability by including offenses like malicious disinformation campaigns, cyberbullying against children, AI-enabled scams, and online impersonation. In addition, the Bill empowers the Ministry of Electronics and Information Technology (MeitY) to identify particular actions as criminal offenses, enabling a faster legal response against emerging threats. This system grants greater ease in dealing with emerging cybercrimes with assurance of severe punishment in case of violation. While the IT Act failed to lawfully define AI-linked harms and disinformation as offenses, the Bill strives to bridge legal loopholes and make the system more enforceable.

13 Amit Singh and Praveen Singh Chauhan, "Navigating Digital Legislation: A Comprehensive Analysis of India's IT Act and Emerging Cyber Security Challenges" (2024) 6(2) *Tec Empresarial* 1 (Costa Rica).

14 M. Pal and M.S. Rana, "Evaluating Intermediary Liability under the Information Technology Act: An Indian Perspective" (2020) 2(2) *Journal of Law and Social Policy* 31.

Regulation of New Technologies

Early in the development of AI, blockchain, and large digital platforms, the IT Act of 2000 created a gap in the regulation of these technologies. The Digital India Bill fills this by establishing special provisions for emerging technologies such as AI, machine learning, and blockchain use. A prime new provision in the Digital India Bill includes penalties for content created by AI that includes the use of deepfakes and the dissemination of misinformation through AI platforms.[15] This would be particularly useful with respect to tools such as ChatGPT, which have advantages but also create threats such as the dissemination of fake information, compromising data privacy, and the creation of biased content.

The Bill aims to control these issues, ensuring the use of AI tools for malicious objectives is prevented while maintaining space for innovation. Moreover, the Bill will likely provide more detailed guidance on the use of blockchain transactions and digital currencies, sectors in which the IT Act had insufficient detailed legal recognition. While the Reserve Bank of India (RBI) had initiated individual cryptocurrency regulations, the Digital India Bill could provide more complete governance over the use of blockchain applications, ensuring greater compliance and stopping fraudulent activities.[16]

The European Union's General Data Protection Regulation

GDPR imposes exact and stringent rules on how data should be treated. It places a strong emphasis on obtaining explicit consent from users, insisting only on the data needed being taken, allowing people to have data removed if they want it gone (right to be forgotten), and maintaining high standards for data handlers. GDPR universally targets any business that processes the information of EU citizens and makes businesses accountable by implementing severe fines for infringements.[17]

15 Mary A. Johnson, "Blockchain Technology and Its Impact on Digital Transactions: A Legal Perspective" (2018) 15(4) *International Journal of Law and Technology* 321.

16 P. Thakur and V. Bansal, "Regulatory Challenges and Implications of Digital Platforms in India" (2019) 10(2) *Journal of Intellectual Property and Competition Law* 134.

17 Sérgio Tenreiro de Magalhães, "The European Union, General Data Protection Regulation (GDPR), Cyber Security Practitioner's Guide" (March 2020) 529–558.

The Digital Personal Data Protection Act, 2023:

The Digital Personal Data Protection Act, 2023 India legislated the Digital Personal Data Protection (DPDP) Act, which resembles the GDPR more than the previous IT Act. The DPDP Act introduces data processing rules based on the consent of the users, the obligations of the data processors, and the rights the users have, such as making a grievance and requesting their data being deleted. Nevertheless, the law makes some exceptions for government entities and relaxes the rules for data being taken outside the nation. The DPDP Act seeks a balance by weighing the aspect of privacy against the national aims of the economy and digital management.[18]

Conclusion

The IT Act has contributed immensely towards the growth of the digital economy in India. It has brought about a legal framework for electronic transactions and given a fillip to establishing confidence in online communication. and transactions. The Act has also supported promoting cybersecurity and data protection, which are essential for growing digital businesses. The Act encompassed any crime that involved a computer or a network found within India, even foreign nationals may be charged so. This legislation lays down the penalties for numerous cyber crimes and fraud in electronic or digital formats. It also gives legality to digital signatures. The Act places emphasis on adopting alternatives to paper-based technology of communication and storing knowledge to facilitate the filing of documents electronically with government agencies, but the IT Act, 2000 is a small step towards preserving data and private information stored through intermediaries in the online database compared to the DPDP Act, Digital India Bill, and GDPR.

The IT Act provides different provisions benefitting the citizen and safeguarding their data

18 Paarth Naithani, "Analysis of India's Digital Personal Data Protection Act, 2023" (2024) *International Journal of Law and Management*, available at https://doi.org/10.1108/IJLMA.

against misuse or destruction. But at the same time, with developments in e-commerce and online trade, there comes a need to tackle issues of such nature as AI and security, discontinued transactions, safekeeping of passwords, cookies, etc. There is a steady rise in cybercrimes which indicates the need for the mechanism to detect and control them.

Nevertheless, there needs to be regular review and refining of the Act to make sure that it stays effective and responsive to the challenge presented by the ever-changing nature of the digital landscape.

References

Kolekar, Y. (2015, May 28). *A Review of Information Technology Act, 2000*. SSRN.

UNCITRAL. (1996). *Model Law on Electronic Commerce with Guide to Enactment 1996*.

Hanna, K. T. (2009). *Definition: Information Technology Amendment Act 2008 (IT Act 2008)*. TechTarget.

Advani, N. (2015). The Evolution of Indian Cyber Law: Past, Present, and Future. *Cyber Legal Studies, 14*, 55.

Press Information Bureau. *Release ID 53617*.

Shreya Singhal v. Union of India, AIR 2015 SC 1523.

Lok Sabha. (n.d.). *Parliamentary Report on the Information Technology Act*.

Columbia Global Freedom of Expression. (n.d.). *Shreya Singhal v. Union of India*.

Singh, J. (2023). What Is 'Overcriminalisation' and How Does the Jan Vishwas (Amendment of Provisions) Bill, 2022 Deal with It? *International Journal of Law Management and Humanities, 6*, 303.

Shreya Singhal v. Union of India, AIR 2015 SC 1523.

Justice K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.

Justice P.N. Varadarajan v. Union of India, (2015) 13 SCC 472.

Singh, A., & Chauhan, P. S. (2024). Navigating Digital Legislation: A Comprehensive Analysis of India's IT Act and Emerging Cyber Security Challenges. *Tec Empresarial, 6*(2), 1.

Pal, M., & Rana, M. S. (2020). Evaluating Intermediary Liability under the Information Technology Act: An Indian Perspective. *Journal of Law and Social Policy, 2*(2), 31.

Johnson, M. A. (2018). Blockchain Technology and Its Impact on Digital Transactions: A Legal Perspective. *International Journal of Law and Technology, 15*(4), 321.

Thakur, P., & Bansal, V. (2019). Regulatory Challenges and Implications of Digital Platforms in India. *Journal of Intellectual Property and Competition Law, 10*(2), 134.

de Magalhães, S. T. (2020, March). The European Union, General Data Protection Regulation (GDPR), Cyber Security Practitioner's Guide.

Naithani, P. (2024). Analysis of India's Digital Personal Data Protection Act, 2023. *International Journal of Law and Management*.