A Comprehensive Overview on the Information Technology Act, 2000: Features and Amendments

Vinod Chawla[1], Dr. Ashok Kumar Yende[2]
[1]*Research Scholar, Bir Tikendrajit University*
[2]*Research Supervisor, Bir Tikendrajit University*

Abstract: ***The Information Technology Act, 2000 grants legal recognition to transactions conducted via electronic data interchange and other electronic communication methods, collectively termed 'electronic commerce.' This act replaces traditional paper-based communication and information storage methods, enabling electronic document filing with government agencies and amending The Indian Penal Code, The Indian Evidence Act, 1872, The Banker's Books Evidence Act, 1891, and The Reserve Bank of India Act, 1934, along with related matters. Cyber law in India primarily focusses on the I.T. Act, 2000, notwithstanding the need for several offences and infrastructure enhancements to be included. In addition, the Act was previously updated in 2008, which included major revisions; yet, this does not alter the reality that technology has advanced considerably since 2008. The Information Technology Act was enacted in October 2000. "As the number of internet users and technological advancements have risen, so too have cybercrimes and criminal methodologies." To prevent such acts and to initiate legal action against them. The IT Act 2008 (Amendment) was enacted to enhance the IT Act and amend the IT Act 2000, addressing gaps and incorporating advancements in contemporary technology. The Information Technology Act 2008 becomes effective in October 2009. The Information Technology Act, 2000 extends across India and also pertains to any act or violation committed outside India by any individual. This research paper provides an overview of the Information Technology Act.***

Keywords: Information Technology Act 2000, Cyber laws, Amendment,cyber-crimes,etc.

I. INTRODUCTION

The Information Technology Act, 2000 ('IT Act') is a comprehensive law enacted to build trust in the digital ecosystem by regulating e-commerce, facilitating electronic filing of documents, and creating criminal offences applicable to the digital ecosystem. Despite amendments in 2009, the IT Act is commonly seen as being outdated.[1]The expansion of the internet and the emergence of various digital technologies in the past decade have prompted numerous enquiries regarding the safety and security of the digital ecosystem, particularly concerning the responsibilities of both government and private sector entities. Reports suggest that the Government of India intends to replace the IT Act with new legislation as part of a comprehensive suite of regulations pertaining to the digital environment.[2] This report attempts to contribute to the process of revision of the IT Act, by examining four critical issues pertaining to the online ecosystem. These are:

- Intermediary liability: There is significant debate globally and in India on the role played by intermediaries in ensuring user safety. At present, the IT Act affords intermediaries protection from prosecution for third party content on their platforms, based on the role played by the intermediary in enabling access to the content, as well as their adherence to due diligence obligations. However, this framework has been criticized for failing to adequately account for the variety of online harms, the role and ability of different intermediaries to address such harms and the

[1] Rishab Bailey, Faiza Rahman, and Varun Sen Bahl, 'Internet Intermediaries and Online Harms: Regulatory Responses' [2020]; Aniruddh Nigam and others, 'Primer for an Information Technology Framework Law' (September 2020); NS Napinnai, 'Cyber security and challenges: Why India need to change IT Act' (February 2017).

[2] Viraj Gaur, 'India Is Moving to Replace Two-Decade-Old IT Act with New 'Digital India Act'' (April 2022); Gulveen Aulakh, 'India to replace IT Act with Digital India Act, part of comprehensive legislative framework expected in 3-4 months' (September 2022).

imposition of broad obligations through the route of due diligence related rules.

- Censorship: The power and processes used to censor digital content in India have been a bone of contention for a number of years. While the digital ecosystem is typically seen as a haven for free speech, the Indian constitutional framework dictates that there must be a method to regulate harmful online content. However, the current framework under the IT Act provides extremely broad powers to the government, with minimal safeguards to fetter abuse.

- Surveillance: The surveillance related provisions in the IT Act were drafted prior to the recognition of privacy as a fundamental right in the Puttaswamy case.[3] It hasbeen argued that the surveillance powers provided to the government are broad, and contain limited safeguards to prevent misuse. At the same time, the growth of digital communication channels and the ubiquity of privacy enhancing technologies such as end-to-end (E2E) encryption has led to a variety of new challenges faced by Law Enforcement Agency (LEA)s in accessing data required for the prosecution of offences.

- Cybersecurity: Ensuring the robustness and resilience of the digital ecosystem is a precondition for growth of this sector. The IT Act establishes institutional frameworks to deal with issues of cybersecurity, though these are said to be ineffective and in need of reform.

All of these concerns are interconnected by a single theme - how can trust be fostered inside the digital ecosystem? Obtaining solutions requires meticulous evaluation of several issues, including national security, public order, the increasing prevalence of online damage, the need to safeguard basic rights, and the promotion of innovation and growth within the digital ecosystem. In the realm of monitoring and censorship, it is essential to consider conflicting constitutional concepts, including privacy, freedom of speech, state security, and public order. Intermediary regulation presents a complex challenge, raising intricate considerations about the capacity of commercial platforms and the government to enhance the safety of the digital environment while fostering innovation. "The topic of cybersecurity similarly prompts enquiries on the responsibilities of the state and private entities in enhancing the security, resilience, and robustness of networks and systems."

[3] Supreme Court of India, ‘Justice K.S. Puttaswamy v. Union of India’ (August 2017).

II.INFORMATION TECHNOLOGY ACT

Prior to the ITA 2000, the ITA imposed stringent restrictions and regulations applicable to cybercafés. The ITA has mandated that cybercafé owners keep a database of internet café customers. The record includes the user's name, contact number, address, system number, and total duration. To facilitate the suspect's traceability. However, the original ITA was hardly impacted, leading to the introduction of a revised statute known as the Information Technology Act 2000, which has several loopholes. The Information Technology Act came into effect in October 2000. ITA 2000 has 13 chapters detailing legislation, sanctions, fines, and offences. Chapter 13 has several parts and subsections that thoroughly elucidate the laws and regulations. The ITA 2000 provisions primarily address e-commerce, digital signatures, associated crimes, and their corresponding sanctions. There are several variants in terminology and the ITA 2008 (amendment) has been enacted. This more explicitly delineates the terms and actions that are unlawful. The Information Technology Act of 2000 does not define cybercrime; it just addresses crimes associated with computers or those perpetrated using electronic means or devices.

Need:

India is the fastest-growing nation in the world and is also seeing technological advancement. Due to the proliferation of technology and activities conducted via electronic mediums, there arose a need for a legal framework that formally recognises criminal acts and provides robust measures against such transgressions. The ITA applies to all Indian nationals, including those residing outside India, for crimes committed inside India from outside. ITA 2000 is the most powerful legislation, comparable to civil law. ITA 2000 facilitates the legal restructuring of transmission over the internet or computer systems. Various kinds of crime are perpetrated. Utilising the internet by those who are either indifferent or unaware of cybercrime and technology. The Information Technology Act of 2000 delineates computer-related offences, including penalties and fines for such crimes.

On May, 2000 the information technology bill was passed by both the house of parliament of India. The Information Technology Act 2000 based on UNCITRAL[4] model law for E commerce. That supports or covers E commerce, E business related issues or unlawful activities. There are 13 chapter and Sub-Sections in Information Technology Act 2000. That describes creation process of Digital signature[5], authentication process, rejection and acceptance of digital signature certificate, duties of subscriber, rules for service provider, cyber offences like hacking, phishing, cyber stalking. Cyberbullying, unauthorised system access, tampering with computer source code, identity theft, and associated offences, along with corresponding penalties and fines. "The penalty for cyber terrorism will be life imprisonment accompanied by a monetary fine." However, the majority of the ITA 2000 pertains to descriptions relating to e-commerce. The ITA 2008 Amendment has undergone several modifications and is devoid of gaps in the Information Technology Act 2000. The Information Technology Act 2008 (Amendment) was enacted in October 2009. This amendment elucidates ambiguous words such as access and network. It also applies certain acts and sections under the IPC or CrPC for offences not specified in the Information Technology Act 2000. Recently, Section 66(a) has been repealed from the ITA 2000; nonetheless, the actions delineated in Section 66(a) will continue to be prosecuted under the IPC or CrPC. Every aspect has both good and negative dimensions. The Information Technology Act of 2000 has both advantageous and deficient aspects that need further implementation.

III. SALIENT FEATURES OF THE INFORMATION TECHNOLOGY ACT, 2000

The salient features of The IT Act, 2000 are as follows –

- Digital signature has been replaced with electronic signature to make it a more technology neutral act.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- It elaborates on offenses, penalties, and breaches.
- It provides for the constitution of the Cyber Regulations Advisory Committee.
- The Information Technology Act defines in a new section that cybercafé is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overridden effect. The provision states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.
- The Information Technology Act is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.

IV. AMENDMENTS OF IT ACT, 2000

With the advancement of time and technology, it was necessary to bring some changes to the Act to meet the needs of society, and so it was amended.

Amendment of 2008:

The 2008 modification modified Section 66A of the Act. This clause was the most contentious since it stipulated the penalties for transmitting inflammatory material via technological means. Any communication or material that incited hate or undermined the integrity and security of the nation was forbidden. Nevertheless, it failed to define the term 'offensive' and the criteria for such statements, resulting in several arrests on this basis. The Supreme Court subsequently invalidated this clause in the case of Shreya Singhal v. Union of India (2015).

An amendment was enacted under Section 69A of the Act, granting the government the authority to block internet sites for reasons of national security and integrity. The authorities or intermediaries may surveil or decrypt the personal information retained by them.

The 2015 Amendment Bill:

The bill was introduced to alter the Act safeguarding the basic rights given by the Constitution to the nation's people. The measure sought to amend

[4] UNCITRAL: The United Nations Commission on International Trade Law.

[5] Digital signature: Electronic signature.

Section 66A, which stipulates penalties for transmitting inflammatory material via electronic means. The clause failed to clarify what constitutes offensive communications and which actions would qualify as the crime. The Supreme Court subsequently invalidated it in the Shreya Singhal case, deeming it a violation of Article 19.

Information Technology Intermediaries Guidelines (Amendment) Rules, 2018:

The government in 2018 issued some guidelines for the intermediaries in order to make them accountable and regulate their activities. Some of these are:

- The intermediaries were required to publish and amend their privacy policies so that citizens could be protected from unethical activities like pornography, objectionable messages and images, messages spreading hatred, etc.
- They must provide the information to the government as and when it is sought within 72 hours for national security.
- It is mandatory for every intermediary to appoint a 'nodal person of contact' for 24×7 service.
- They must have technologies that could help in reducing unlawful activities done online.
- The rules also break end-to-end encryption if needed to determine the origin of harmful messages.

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

In 2021, the Indian government set certain regulations for intermediaries to adhere to. The regulations mandated that intermediaries operate with due diligence and designate a grievance officer. They were also mandated to establish a Grievance Appellate Tribunal. All customer concerns must be addressed within 24 hours and handled within 15 days. It also offers a 'Code of Ethics' for those disseminating news and current events, making it contentious. Numerous individuals contend that the regulations restrict freedom of speech, expression, and the press.

The intermediaries were mandated to provide information and particulars of a suspected user to the government if there was any danger to national security and integrity. Consequently, writ petitions were submitted to many high courts challenging the regulations. Recently, the Bombay High Court issued a stay in the cases of Agij Promotion of Nineteenonea Media Pvt. Ltd. vs. Union of India (2021) and Nikhil Mangesg Wagle vs. Union of India (2021) concerning two sections of the laws pertaining to the Code of Ethics for digital media and publishers.

Objectives of the Amendments in The Information Technology Act, 2000:

- A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, ecommerce frauds like personating commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal Code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes.
- With proliferation of information technology enabled services such as egovernance, e-commerce and e-transactions, protection of personal data and information and implementation of security practices and procedures relating to these applications of electronic communications have assumed greater importance and they require harmonization with the provisions of the Information Technology Act. Further, protection of Critical Information Infrastructure is pivotal to national security, economy, public health and safety, so it has become necessary to declare such infrastructure as a protected system so as to restrict its access.
- The service providers may be authorized by the Central Government or the State Government to set up, maintain and upgrade the computerized facilities and also collect, retain appropriate service charges for providing such services at such scale as may be specified by the Central Government or the State Government.
- The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures. The General Assemblyof the United Nations by its resolution No. 56/80,

dated 12th December, 2001, recommended that all States accord favorable consideration to the said Model Law on Electronic Signatures. Since the digital signatures are linked to a specific technology under the existing provisions of the Information Technology Act, it has become necessary to provide for alternate technology of electronic signatures for bringing harmonization with the said Model Law.

V. CONCLUSION

Today, we are all immersed in the realm of the internet. As internet speeds increase, individuals choose virtual transactions over real ones. Nevertheless, government initiatives like the Digital India Program have encouraged the use of digital payments, which represent a significant security danger. "While the internet has proven beneficial during catastrophes such as COVID-19, it is important to acknowledge the concurrent rise in internet-related offences and crimes." It is important to understand the laws regulating cybersecurity. The Information Technology Act of 2000 delineates different offences pertaining to data breaches and individual privacy, stipulating corresponding punishments or penalties. It also addresses intermediaries and governs the authority of social media. The advent of technology and e-commerce has led to a significant rise in cybercrimes and offences pertaining to data and genuine information. The data concerning national security and integrity was compromised, prompting the government to restrict social media activity and the data contained inside. The Act is a measure to safeguard data and sensitive information held by internet intermediaries. It provides many safeguards that safeguard people and secure their data from abuse or loss. Nonetheless, with the progression of e-commerce and online transactions, it is essential to address issues such as internet speed and security, interrupted transactions, password safety, cookies, and related concerns. The incidence of cyber-crimes is growing rapidly, necessitating the establishment of a system for detection and control.

REFERENCES

[1]. Cyber Security, Understanding Cyber Crimes, Computer Forensics and Legal Perspectives.

[2]. Dennis, Michael Aaron, Cybercrime, Encyclopaedia Britannica, (19 Sep. 2019), https://www.britannica.com/topic/cybercrime.

[3]. Henry et al, Countering the Cyber Threat, 3 no. 1 The Cyber Defense Review, 47–56 (2018).

[4]. India: Promoting internet safety amongst 'netizens', UNODC (United Nations Office on Drugs and Crimes), https://www.unodc.org/southasia/frontpage/2012/May/india_- addressing-the-rise-of-cybercrime-amongst-children.html

[5]. Information Technology Act: In Depth Analysis of Indian IT Act Related to Unauthorized Access.

[6]. Jigar Shah, A Study of Awareness About Cyber Laws for Indian Youth, 1(1) International Journal of Trend in Scientific Research and Development, (2016).

[7]. Kshetri, Nir, Diffusion and Effects of Cyber-Crime in Developing Economies, 31 no. 7 Third World Quarterly, 1057–1079 (2010).

[8]. Prof. Dr. Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response, Telecommunication Development Sector (ITU, 2014).

[9]. Shubham Kumar et al, Present scenario of cybercrime in INDIA and its preventions, 6 no. 4 International Journal of Scientific & Engineering Research, 1971 (2015).

[10]. The Information Technology Act, 2000: Bare Act by Universal Publication.