MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 2178-2180

Role of The Information Technology Act, 2000 In Tackling Online Fraud

Mariya Khan[1], Sunil Kumar Sharma[2]
Institute of Legal Studies & Research, Mangalayatan University, Beswan, Aligarh, Uttar Pradesh-202146 [1,2]
Email- 20221414_mariya@mangalayatan.edu.in[1] ,
sunil.sharma9590@mangalayatan.edu.in[2]

ABSTRACT
As access to the internet expands quickly across India, online fraud, scam and identity theft (in addition to other cybercrimes), has been on the rise. The Information Technology Act, 2000 has rapidly developed as India's primary statutory law to address cybercrime. Organizations are vulnerable to cybercrime which deals with, rather than warnings, Indian Cyber Law ensure corporations are engaged regarding compliance. This paper assesses how far the Act has come in vertical and budding cyber threats and defines the limitations, where relevant, of rules such as the Information Technology Rules, 2021 and preliminary data protection efforts. The aim of this paper is to captures case studies around notable events, institutional efforts such as CERT-In and reporting channels for cybercrime by the government; in order to evaluate read what improvise (e.g. lessons learned) and lack thereof in relation to cyber law enforcement progress in India. The paper will end with tangible recommendations for implementing the law and informing the public in regards to legal compliance to reduce online fraud and improve security.

Keywords- Cybercrime Regulation; Information Technology Act, 2000; Online Financial Fraud; Section 66D; Phishing; Identity Theft; Digital Governance; IT Rules 2021; Data Protection Laws; Cyber security in India.

I. INTRODUCTION
In last ten years, India has gone through a unique and digital revolution, catalyzed by penetration of internet, smartphones affordability and strong government outreach and frameworks (like the Digital India Program). Digital transformation is now being witnessed in many key sectors such as banking, commerce, education, healthcare, and public services and it has allowed people to access resources and information faster and quicker. But, with the digital growth came new and evolving types of threats most notably a rise in online frauds and cybercrimes. In India, online fraud is posed in various sophisticated forms, from phishing schemes that deceive users into divulging private information, to a multitude of identity thefts, OTP based scams, and fake websites and apps designed to look like various legitimate services. These crimes present a significant risk to individual users and are an equally marked risk to the structure of our country's digital backbone.

In response to these challenges, the Government of India introduced the Information Technology Act, 2000, which was a landmark contribution to the development of cyber law in the country. It was conceived to provide the legal basis to protect electronic transactions, as well as providing legal aspects to data security and regulating the world of cyber as a whole. It security and regulating the world of cyber as a whole. It provided legal recognition of electronic records and digital signatures as well as provided both a legal framework for security and criminally recognized a vast class of cyber offences, including those associated with identity fraud or unauthorized use of sensitive information. The main objective of the IT Act is to create a secure and trusted information technology domain by deterring inappropriate or fraudulent use of information technology. Because of the dynamic nature of cyber criminality, the IT Act has seen a number of amendments since the IT Act came into force and has often resulted in further rules and Guidance being introduced (examples include IT Rules, 2021 etc.). The IT Act is still very relevant in protecting citizens and businesses today and into the future from any potential threats from cybercrime; as well as building and maintaining trust and confidence with respect to the digital economy in an increasingly 'digital first' world.

OBJECTIVES
1. To Provide Legal Recognition to Electronic Transactions and Digital Signatures:-
The purpose of the Act is to recognize the legal status of electronic records and digital signatures and provide for using digital means to transact business and engage in official communications as opposed to semi legal paper-based methods.

2. To Define Cybercrimes (e.g., hacking, identity theft, data breach); to provide legal penalties for those crimes:-
The Act goal is to provide clarity regarding types of various forms of cyber offences and the legal consequences that flow from those offences, which will deter further malicious activity in cyberspace.

3. To Protect Integrity and Security of E-commerce and Digital Payment Mechanisms:-
The Act proposes to promote online trust in electronic commerce by instituting electronic financial transactions, exchanges of an appropriate and effective nature, and predictable legally enforceable rights and obligations.

4. To Equip Law Enforcement with the Legal Means to Investigate and Prosecute Cyber Crime:-
The Act intends to provide a level of procedural measures so law enforcement will be able to detect, investigate and prosecute cyber related crimes.

II. KEY PROVISIONS RELATED TO ONLINE FRAUD
a. Section 66 – Computer-Related Offences - Section 66 sets out a number of offences consisting of assaulting

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 2178-2180

computers or computer systems. It provides a penalty to person who, dishonestly or fraudulently, does any act described in Section 43 - which includes things like unauthorized access, stealing data, or putting harmful code (like viruses) on a computer system and sending offensive or misleading messages by way of a communication service (this includes email, messaging apps, and social media).

Penalty: Offenders of this offence (under Section 66) may face imprisonment for term up to three years, or a fine up to ₹5 lakh (the allowed fine will depend on the severity and extent of the offence).

b. Section 66C – Identity Theft –This section relates specifically to the crime of the dishonest or fraudulent use of another person's electronic signature, password or other unique identifying particular; for instance, if a person commits fraud using someone else's Aadhaar details, email username and passwords or banking passwords, then, Section applies.

Penalty – the punishment is imprisonment for 3 years and/or fines not exceeding ₹1,00,000.

c. Section 66D – Cheating by Personation using Computer Resources - Section 66D is for where a person cheats another person through personation of someone else using computer resources i.e., computer resources means all of online digital space and space where digital computing occurs, so includes internet meeting mobile communications. The section mainly applies to phishing attacks, fake job portals, bogus lottery scams, and similar variety of place based scams via electronic means where they may personate others in their scams.

Penalty – the person convicted will be liable to be punished with 3 years, and/or fines which may extend to ₹1,00,000.

d. Section 43- Penalties and Compensation for unauthorized access and damage to Computer, Computer Systems, etc.

Section 43 outlines breaches of computer systems which embrace what might be appertained to as hacking or penetration, involvement with contagions or malware attacks, destroying or altering information without concurrence, disturbance to services, theft and copying of defended records and data. It should be directed out this section is civil and not lawless and does not give for imprisonment but compensating the dissatisfied person's damage. Remedy The dissatisfied person can sue to have fiscal compensation for the damage he or she has suffered from the malefactor, but compensation will be restored rested on the loss and that damage suffered.

e. Section 72 – penal provisions for Breach of Confidentiality and Privacy - Section 72 creates a penalty for a person who obtains access to any electronic record, personal data, or confidential information while exercising powers under the Act, and discloses (or uses) information which he or she is not entitled to do so. Section 72 applies specifically to government officials, service providers or those entrusted with sensitive digital information.

Penalty: A person who breaches confidentiality is punishable with imprisonment or a fine, or both. Specifically, the criminal penalties are imprisonment up to two years, or a fine up to ₹1 lakh, or both.

III. THE ROLE OF THE ACT IN PREVENTING DIGITAL FRAUD

- **Legal Deterrence:** The IT Act specifies punishments for digital fraud and unauthorized use of internet platforms.
- **Lots of power to investigate:** The Act grants law enforcement, the Cyber Cells and others the powers to investigate and prosecute on-line fraudsters.
- **Judicial powers of e-friction:** Distinctively Cyber matters are heard by designated Adjudicating Officers and Cyber Appellate Tribunals.
- **Data Security Compliance:** The Act pushes digital service providers to comply with data security due diligence requirements.
- **Commerce Transaction Protection:** The regulation of a single regulatory framework for digital avenues of commerce and e wallets for the protection or mitigation of transaction costs.

IV. LIMITATIONS AND CHALLENGES

- **Under reporting of crimes:** Victims may fail to report an offense because they do not know about their options, or because they fear the offender may retaliate against them.
- **Jurisdiction:** Cyber fraudsters are multi-jurisdictional criminals as they often operate across states and national barriers.
- **Lack of professional investigative teams**: Half of the police stations in India still do not have specialized cybercrime investigators.
- **Length of judicial process:** Cyber-crime cases are protracted due to delay, the time process of procedural delays, and in the end very low conviction rates.
- **Insufficient Data Protection along with information technology:** There is no statutory data protection law in India working in conjunction with the IT Act.

V. RECENT DEVELOPMENTS AND AMENDMENTS IT RULES, 2021 (CENTRAL GUIDELINES AND DIGITAL MEDIA ETHICS CODE)

Social media intermediaries and digital platforms must now respond expeditiously to complaints. Tougher obligations for removal of dangerous content and guarding druggies against online frauds. Digital Personal Data Protection Act, 2023 (Alongside Legislation) Although this act is not a part of the IT Act, it addresses some important privacy and data handling issues that are also frequently at the heart of online frauds.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 35 Issue 2, 2025, Pages: 2178-2180

- **The action to be taken by Government and Agencies – CERT-In (Indian Computer Emergency Response Team):** watches for incident pre-emptively "on the sidewalk", and constantly monitors and responds to cyber security incidents; Cyber Crime Reporting Portal (www.cybercrime.gov.in). Now, online governments are actually not just promoting but enabling online fraud.
- **RBI Guidelines:** The Set of Regulations / guidance on how banks and payment systems detect and prevent fraudulent digital transactions.

❖ **CASE STUDIES**

✓ **Case 1: State of Maharashtra v. Nikita Sharma (2020)**
The accused impersonated a bank officer and deceived a victim to the extent of ₹2.5 lakh (OTP already fraud). The court held this under Section 66D of the IT Act and IPC 420 (cheating).

✓ **Case 2: Sanjay Kumar v. State of Delhi (2022)**
A fake job portal collected user data and exploited them for money. Police used digital tracking and logs from social-media using the provisions of Section 66C/66D to arrest the fraudster.

VI. SUGGESTIONS

- Raise unease around rural cybercrime.
- Improve the claims process for victims so that better systems are in place for communication, and that the claims forms are easy to fill in, as well as importantly, get back to them quickly after an initial submission.
- Improve programs around education directly relating to rural cybercrime.
- Educate people living in rural areas about the abuse of cyber spaces, and the way to collectively advertise anonymously in conjunction with scam culture.
- Encourage good cyber hygiene respect to aspects of usable space and cyber connectivity for the purpose of feedback in the context of forming new behaviors and habits. Recommended works would be the use of passwords on devices, two-factor authentication, and to not share variable(s) like one-time passwords.

VII. CONCLUSION

The Information Technology Act, 2000 serves as the primary cyber law framework in India and is important to the fight against online fraud. Although the act creates a good framework from which to prosecute malicious activity, the evolution of cybercrime means ongoing updates, improvements in cyber awareness, and improved coordination between technology platforms, the legal system, and the consumer is crucial.

REFERENCES

[1] Kumar, R. (2021). Tackling cyber fraud through legal reform: Evaluating the IT Act in the digital age. Cyber Law Review, 7(1), 89–103.
[2] Singh, A. (2022). Addressing digital fraud in India: A study of the IT Act, 2000 and its effectiveness. Indian Journal of Law and Technology, 18(2), 145–162.
[3] Indian Computer Emergency Response Team (CERT-In). (2023). Cyber security framework and guidelines. Ministry of Electronics and Information Technology.
[4] Press Information Bureau. (2023). Government initiatives to tackle cybercrime and fraud. Ministry of Home Affairs.
[5] Reserve Bank of India. (2023). Master directions on digital payment security controls.
[6] Government of India. (2000). The Information Technology Act, 2000. Ministry of Law and Justice.