Issue Brief

March 2025
No : 424

Review of Information Technology Act 2000 (IT Act, 2000)

Brigadier Saurabh Tewari, (Retd)

Review of Information Technology Act 2000 (IT Act, 2000)

Brigadier Saurabh Tewari (Retd)

Abstract

The Information Technology Act 2000 (IT Act-2000) was approved in June 2000 by the President and came into effect from 17 October 2000. Post its enforcement, it underwent two major changes—one in 2008 and the next in 2018. Use of new technologies like Artificial Intelligence (AI) in the execution of cybercrimes as well as other technological advancements have made the digital world more prone to misuse. Realising its intensity, the Government of India is in the process of drafting a new legislation— the Digital India Act. This paper intends to review the IT Act (2000) and the rules/guidelines issued under the aegis of same, to identify grey areas and voids that may be considered for inclusion in the proposed legislation.

Keywords: IT Act 2000, Electronic Records, Digital Signature, Electronic Signature, Cyber Incident, Cybercrime, Computer Emergency Response Team (CERT), National Critical Information Infrastructure Protection Centre (NCIIPC), Deep Fake, Quantum Computing, Cryptocurrency, Digital Arrest, Ransomware.

Introduction

Evolution of Cyber Law in India

The UN General Assembly (UNGA) passed a resolution in January 1997 for adoption of a Model Law on E-Commerce, which emphasized that all Nation States should frame cyber laws of their own. As a result of this resolution, the Department of Electronics, Government of India, drafted the Information Technology (IT) Act which was put up to the Parliament of India in 1999 by the newly formed Ministry of IT.

After making some changes as recommended by the Ministry of Commerce, the final draft was prepared by the Law Ministry and put up to the Parliamentary Committee. After the Committee's approval, the Bill was produced for approval of both the Houses on 17 May 2000. Thus, the IT Act2000 (Act 21 of 2000), came into being and became effective from 17 October.

Purpose of the Act

The purpose of the IT Act is "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication" (IT Act 2000, p.1). The Act primarily deals with legal recognition of electronic records, digital signatures, cybercrimes & punishments and cybercrime adjudication issues.

Jurisdiction

The IT Act 2000 is applicable within India and also outside of India for any offences listed therein" (IT Act 2000, p.1).

Structure of IT Act 2000

The Act is divided into 13 chapters and 94 sections. It covers various aspects related to e-commerce transactions, cybercrimes, penalties, adjudication powers, regulatory authorities, etc. Chapter-wise layout of IT Act 2000 is given below:

- Chapter 1 gives definitions of certain relevant terms.
- Chapter 2 deals with digital signatures and electronic records authentication.
- Chapter 3 discusses the provisions related to e-governance like legal sanctity of electronic records and documents, electronic contracts, etc.
- Chapter 4 deals with the attributability of electronic records.
- Chapter 5 dwells on aspects like secure electronic records and secure digital signature.
- Chapter 6 gives details of the regulatory ecosystem.
- Chapter 7 deals with issuance, suspension and revocation of digital signature certificates.
- Chapter 8 deals with duties of digital signature certificate subscribers.
- Chapter 9 deals with certain penalties and adjudication issues.
- Chapter 10 gives details of appellate authorities.
- Chapter 11 gives offences and penalties.
- Chapter 12 gives details of service provider liabilities.
- Chapter 13 gives details of the powers of various government functionaries.

Certain important cybercrime offences include "impairment to computer system, interfering with computer documents, hacking into computers, publishing of obscene electronic information and illegal access to protected systems". (IT Act 2000, pp.14-20).

First Amendment: 2008

The IT (Amendment) Act 2008 was published on 05 February 2009. Some important amendments that were brought about through this Act are as under:

"Digital Signature" was substituted with "Electronic Signature". This was done to ensure a 'Technology Agnostic' framework.

Certain additional terms were defined, and few were modified like Communication Device, Cyber Café, Cyber security, Electronic Signature, Electronic Signature Certificate and Computer Source Code {IT (Amendment) Act 2008, p.6}.

Section 10A was introduced to provide legitimacy to digital contracts {IT (Amendment) Act 2008, p.4}.

In section 43, the compensation limit of Rs One Crore was removed. Additional penalties were laid down like imprisonment up to 3 years and fine up to Rs 5 lakhs. Additionally, section 43A was introduced to include mishandling of personal data by businesses. {IT (Amendment) Act 2008, p.6}. New sections viz. 65A and 65B were added to modify the Indian Evidence to allow for legal recognition of electronic evidence. Additional sections viz. 66A-F were inserted to include cybercrimes related to misinformation, use of stolen computers, fake use of electronic signatures, impersonation, privacy violations, interruption of critical services and cyber-terror. Sub section 67B was added to explicitly include offences connected to child pornography. {IT (Amendment) Act 2008, pp.9-11}.

Second Amendment:2018

The IT (Amendment) Bill 2018 was published in the Gazette of India on 27 November 2018 as an amendment to IT Act 2000. Vide this amendment, Section 66A was deleted from the Act as per orders of the Supreme Court {IT (Amendment) Bill 2018}.

Section 66A criminalized sending of offensive messages through electronic means. This section was purported to be misused especially by the government agencies to stifle free speech, and hence the Supreme Court decided to strike it down.

Rules/ Guidelines Issued Under the Aegis of the IT Act 2000

Certain Rules/guidelines have been issued under the aegis of the IT Act ,2000. Important ones are discussed in succeeding paras.

IT Rules- 2011

These Rules were issued to safeguard handling of sensitive information of customers/ employees by corporate houses in a legal and accountable manner. It also gives supplementary definitions which are not given in the IT Act 2000 like Biometrics, Body Corporate, Cyber Incidents, Password, Personal Information, Sensitive personal data or information (IT Rules 2011).

NCIIPC Guidelines- 2015

The *National Critical Information Infrastructure Protection Centre (NCIIPC)* issued these guidelines in January 2015, which are "intended to assist and advice the management and Chief Information Security Officer (CISO) of the Critical Sectors regarding the infrastructure, manpower, skill and guidelines required in meeting the ever growing and challenging task of the protection of their respective CIIs in consultation and coordination with NCIIPC" (NCIIPC Guidelines,2015, p.22).

Seven sectors have been nominated as CII in India——Banking, Financial Services & Insurance (BFSI), Government, Health, Power & Energy, Strategic & Public Enterprise, Transport, and Telecom (NCIIPC website).

NCIIPC Rules-2018

These rules were issued on 01 June 2018 with an aim to lay down the “Information Security Practices and Procedures for Protected System” (NCIIPC Rules,2018).

Directions CERT-In: 2022

These directions were issued by CERT-In on 28 April 2022 (effective from 28 June 2022). Important aspect of these directions are given below:

- All entities like service providers, data centres, government bodies (corporates and intermediaries) are required to link up with the Network Time Protocol (NTP) server of the National Informatics Centre or the National Physical Laboratory.

- All types of cyber incidents need to be informed to CERT-In within maximum six hours of manifestation.
- All entities mentioned above are required to appoint a single point of contact for interfacing with CERT-In (Directions: CERT-In, 2022).

Analysis

Analysis of the IT Act, 2000

On analysis of the IT Act,2000 (including amendments) and the rules/guidelines, some major issues emerge that needs to be addressed in the right earnest. The Government is preparing to launch a new legislation to replace the IT Act,2000 called the "Digital India Act". The issues discussed below may be considered to be mitigated through the new legislation:

- There is critical need for a holistic review of the IT Act,2000 to ensure that it is future proof and technology agnostic. Technology in IT domain is evolving very rapidly and bringing new dimensions to fore. Cybercriminals are exploiting these technologies and inventing novel ideas about execution of cybercrimes. Things like 'deep fake videos' and 'voice cloning' using AI are opening new frontiers of challenges. New types of cybercrimes like digital arrest, ransomware, sextortion, cryptocurrency crime, etc. are on the rise. A comprehensive review is therefore needed to align the legal framework with the new age technologies and new age cybercrimes. In fact, regulatory framework should, as far as possible, be technology neutral— it can then sustain for a long time without the need for frequent revisions.
- Another issue with the IT Act ,2000 is that it is not a law by itself but relies on the Indian Penal Code (now *Bhartiya Nyaya Samhita*- the BNS-2023) and also no new offences have been added after 2008. Apropos, the IT Act, 2000 needs a holistic review afresh. Cybercrimes in India requires an exclusive cybercrime law and not just a chapter in an e-commerce legislation. (Dr. Pavan Duggal, Cybercrime Lawyer, Supreme Court of India; personal interview; 30 Aug 2024).
- A major change that was brought about in the amendment of 2008 was that, all offences wherein imprisonment was up to three years, were made bailable. This resulted in reduction in deterrence to the cybercriminals and consequently the conviction rates also dropped as bail provides an opportunity to the accused to

go out and tamper with the evidence. This issue needs to be addressed, while at the same time striking the balance to avoid resulting in a draconian law. (Dr. Pavan Duggal, Cybercrime Lawyer, Supreme Court of India; personal interview; 30 Aug 2024).

- After deletion of Section 66A of the IT Act 2000, there is no specific provision in the Act that deals with the crime related to cyber defamation.
- IT Rules,2011 provides a workable structure for collecting, handling and revelation of digital personal data; however, following are the grey areas:
    - Important information like date of birth, PAN/AADHAAR number, details of family members, contact details, address, etc. have not been included in the definition of personal data.
    - No penalties are laid down for violations.
    - The definition of "Cyber Incident" provided in IT Rules, 2011 and CERT-In Rules,2013 are different. These kinds of situations are not good from legal standpoint and offer legal loopholes to cybercriminals.
    - Certain critical sectors that may be considered for being declared as CII (in addition to those already declared) are Aviation, Cloud & Data Centre Services, Defence Industry, Emergency Services, Energy, Food & Agriculture, Nuclear, Operational technology (OT)[1], Shipping, Space and Water/Sewage & Dams.
- There are no penalties specified in the NCIIPC Rules, 2018 for any violations. Penalties are important to set deterrence and ensure compliance.
- Timeline of six hours to report a cyber breach to the CERT-In is impractical. It may generate false positives also. A more reasonable time needs to be given to the infrastructure owner to decide on the nature of attack and then report it to the concerned government authorities.

Conclusion

The IT Act, 2000 (and amendments) has served the government good for long, but it is time for a major review now. This becomes even more important in the context of advent of new emerging technologies and concepts like AI, block chain, quantum computing,

[1] OT is a group of technologies that are used to interconnect physical systems with network and protocols to effect industrial control operations. Examples of OT includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), etc.

cryptocurrency, internet of things, etc., which are not only providing the cybercriminals with a larger canvas to commit cybercrimes, but are also giving rise to new types of cybercrimes like digital arrest, ransomware, deep fake videos, use of AI to create phishing emails, voice cloning, etc. Further, in line with the global practice, it is time to have a dedicated legislation on cybercrime rather than just having a chapter on cybercrime in a larger regulatory document on e-commerce ecosystem.

Works Cited

Directions CERT-In, (2022). https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf.

IT Act2000. https://www.meity.gov.in/writereaddata/files/ itbill2000.pdf.

IT (Amendment) Act 2008. https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf.

IT Rules 2011 {Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011}. https://www.meity.gov.in/writereaddata/files/GSR313E10511%281% 290.pdf.

IT (Amendment) Bill 2018. http://164.100.47.4/billstexts/lsbilltexts/asintroduced/2127as.pdf.

NCIIPC Guidelines 2015 (Guidelines for the Protection of National Critical Information Infrastructure). http://nciipc.gov.in/documents/NCIIPC_Guidelines_V2.pdf.

NCIIPC Rules 2018 {Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018}.https://www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf.

About the Author

Brigadier Saurabh Tewari, a retired Indian Army officer with over 35 years of distinguished service, specializes in IT/Telecom network design, cyber security, and project management. Brigadier Tewari considers himself an academician in uniform. He is a Gold Medalist from IIT Delhi and M. Phil from Pune University. An avid researcher, he has to his credit two books on military technology & multiple research papers and is currently pursuing PhD in cybercrime & cyber security.

During his Army service, Brig Tewari has been fortunate to have a teaching experience of four years with B. Tech students and Defence & Strategic Studies students, as also handling administration of an educational institute for about two years.He has led major defence IT/telecom projects while in service and is widely recognized for his contributions to military technology with specific reference to ICT and cyber security. Currently, he serves as an Advisor at Army HQ, continuing to lend his expertise to defence communications and security.

Brigadier Tewari has vast operational experience and has served in Sri Lanka during Operation Pawan (in 1988-89) and was posted in the Ladakh sector during Operation Vijay, the Kargil war (in 1999). In addition, he has also served in counter insurgency affected areas in Assam, Punjab and the highest battlefield in the world, the Siachen Glacier. In keeping with his penchant for academics, Brig Tewari has also completed a PG diploma in Management, Diploma in Cyber Law and a Certificate in Cyber Diplomacy from the United Nations.