KNOWLEDGE BANK™
Always stay curious

MCO LEGALS

17th DECEMBER, 2021

SERIES ON CYBER LAW: ISSUE 1

A COMPREHENSIVE ANALYSIS OF INFORMATION TECHNOLOGY ACT, 2000

Amit Meharia

Managing Partner, MCO Legals
LLB (Hons)
King's College London, Solicitor
(Supreme Court of England & Wales)

Expertise:

Corporate Due Diligence &
Corporate/Commercial Arbitration

amit.m@mcolegals.co.in

Bhavna Sharma

Research Partner

B.Sc., LLM,
Research Scholar
RML National Law University
Lucknow

INTRODUCTION

In 1996, the United Nation Commission of International Trade Law (UNCITRAL) came up with the Model Law on e-commerce to meet the growing needs and challenges of the technologically driven business sector. Subsequently, owing to extensive digitalization in the trade activities globally, the General Assembly of United Nations recommended all member States of the United Nations to persuade the model and provide recognition to electronic records and electronic transactions.

Henceforth, India introduced the Information Technology Act, 2000 (The Act) which came into effect on 17th October, 2000. It is one and the only legislation dealing with cyber regulations and e-commerce in India. The major purpose of this legislation was to lay down a legal framework to deal with the e-commerce activities, e-governance, electronic records and signatures and other associated subject matter.

Objective of the Act-

The objective of the act is "*to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto*."

Salient features of the Act –

• The act is divided into 13 chapters, 4 schedules and 94 sections. Each chapter is exclusively allocated to a separate concept.

• The first chapter of the Act has provided a comprehensive list of various definitions of several terms used in the Act. It also mentions that the act extends to whole of India except negotiable Instrument Act, power of attorney, trust, will and any contract of sale or conveyance of immovable property. This act also applies to any offence committed by any person outside India.

•The Act brought amendment to Indian Penal Code, 1860, Indian Evidence Act, 1872 the Bankers Book Evidence Act, 1891 and Reserve Bank of India Act, 1934.

• Chapter 2 of the Act provide authentication to electronic records and authentic signature. A subscriber is a person in whose name the digital signature certificate is issued. Any subscriber may authenticate an electronic record by affixing his digital signature. The authentication of the electronic record is effected by the use of asymmetric crypto system and hash function. (Section 3)

• Chapter 3 of the Act is dedicated to Electronic Governance in which it provides legal recognition to electronic records and electronic signatures and promoted the use of both in the governmental functioning. The Central Government is empowered to make rules and regulations regarding the type, manner, format, procedure, control or any other matter related to digital signatures. (Section 10)

• A "certifying authority" is appointed under chapter 6 of the act. The Central Government shall appoint a Deputy Controllers and Assistant Controller as per requirement. Few major functions of the Controller are supervising the certifying authorities, certifying public keys, specifying the qualifications and experience which employee of the certifying authorities should possess, resolving any conflict of interest between the certifying authorities and the subscribers, facilitating the establishment of any electronic system by a certifying authorities, deciding the conduct of the certifying authorities, etc. A Certifying Authority is empowered to issue a Digital Signature Certificate which includes powers related to issuance, suspension and revocation.

• Duties of Subscribers are provided under Chap-

ter 8 of the Act. Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key and prevent its disclosure to any unauthorised person.

• Chapter 9 deals with Penalties and Adjudication. It is one of the eminent chapters of the Act. Penalty is attracted where there is any damage to computer, computer system or computer network, etc. A compensation of maximum One Crore rupees can be imposed upon the offender. Under section 44, penalty is also stipulated for when any person fails to furnish information which he is bound to furnish under this to computer, computer system or computer network, etc. A compensation of maximum One Crore rupees can be imposed upon the offender. Under section 44, penalty is also stipulated for when any person fails to furnish information which he is bound to furnish under this act. A maximum penalty of 5000 rupees is imposed for every day during which such failure continues.

Section 46 of this chapter states the power of adjudication. It says that when there is any contravention of the provisions of this act and any penalty is attracted, the Central Governments appoints an adjudicating officer who is not below the rank of Director of the Government of India or State Government on equivalent positions for holding an inquiry in the matter. Such Adjudicating officer should possess relevant experience in the field of information technology and legal/judicial experience. The pecuniary jurisprudence of the adjudicating officer is to only deal with claims for injury or damage not exceeding five crore rupees. The adjudicating officer shall exercise jurisdiction in respect of contravention in relation to Chapter 9 and no other. It is provided that every application before the adjudicating officer shall be heard and decided in four months and the whole matter in six months.

• Chapter 10 deals with Cyber Regulations Appellate Tribunal. Establishment of Cyber Appellate Tribunal is provided under section 48 of the Act. As its name suggest, it only has appellate jurisdiction. An appeal shall lie before it from the order of the Controller of certifying authorities or adjudicating officer. A person appointed as a chairperson of a cyber-appellate tribunal should be qualified to be judge of High court or holds or has held that position. The order of such chairperson shall be final and not to be called in question on the ground merely of any defect in the constitution of Cyber Appellate Tribunal. The tribunal shall vest with the same power as of the civil court.Any person aggrieved by the decision of the Cyber Appellate Tribunal may file an appeal before the High Court.

• Following are the cyber offences covered under Chapter 11 of the act − tampering with computer source document, sending offensive messages, identity theft, impersonation, violation of privacy, cyber terrorism, publishing or transmitting obscene material or sexually explicit content, pornography, etc. The punishment for each offence varies depending upon the nature of offence. The offences punishable with imprisonment of three years and above are considered cognizable and bailable irrespective of Code of Criminal Procedure. Only a police officer not below the rank of Inspector shall investigate any offence under this chapter.

• Chapter 12 deals with liability of Network Service Providers.Section 79 of this chapter exempts intermediaries from the liability for any third party information made available or hosted by him. There are certain conditions to avail this safe harbour such as the intermediary itself does not initiate the transmission, select the receiver or modify the information. It observes due diligence while discharging its duties. It should only act as an intermediary and provide access to a communication system. The intermediary shouldn't have conspired, abetted or aided in the commission of prohibited act.

All been said and discussed, it is beyond doubt that the Information Technology Act, 2000 is a blossoming step towards controlling and regulating the digital sector. This act was specifically brought to legalise electronic records and regulate e-commerce business. The legislator didn't think 22 years back such wide spread of technology touching nearly every sector may it be education, entertainment, global economy, financial, business, etc. and resulting in cyber crimes, irregularity and turmoil in the cyberspace. Hence, currently this act is somewhere failing to combat the demands of the contemporary world and needs to be amended. The last amendment was in 2008 and now its high time for redrafting this Act taking account of the new developments in the technology belt and mounting number of cyber crimes.