An Overview of Information Technology Act, 2000

This article written by Avani Yadav gives a gist of The Information Technology Act, 2000. However, the main motive of this Act is to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly known as E-commerce.

Introduction Of The Information Technology Act, 2000

The Information Technology Act, 2000 provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as"electronic commerce", which involves the use of alternatives to paper-based 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 Books Evidence Act, 1891 and The Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.
The Information Technology Act, 2000 extend to the whole of India and it applies also to any offence or contravention thereunder committed outside India by any person.

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 elaborates on offenses, penalties, and breaches.
- It outlines the Justice Dispensation Systems for cyber-crimes.
- The Information Technology Act defines in a new section that cyber café 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 provides for the constitution of the Cyber Regulations Advisory Committee.
- 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.
- It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

Application of The Information Technology Act, 2000

Nothing in The Information Technology Act, 2000 shall apply to documents or transactions specified in the First Schedule: Provided that the Central Government may, by notification in the Official Gazette, amend the First Schedule by way of addition or deletion of entries thereto. Every notification issued shall be laid before each House of Parliament.
Following are the documents or transactions to which the Act shall not apply −

- **Negotiable Instrument**(Other than a cheque) as defined in The Negotiable Instruments Act, 1881;
- A **power-of-attorney** as defined in The Powers of Attorney Act, 1882;
- A **trust** as defined in The Indian Trusts Act, 1882;
- A **will** as defined in The Indian Succession Act, 1925 including any other testamentary disposition;
- Any **contract** for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as maybe **notified by the Central Government.**

Amendments Brought in The Information Technology Act, 2000

The Information Technology Act, 2000 has brought amendment in four statutes vide section 91-94. These changes have been provided in schedule 1-4.

- The first schedule contains the amendments in the Penal Code. It has widened the scope of the term "document" to bring within its ambit electronic documents.
- The second schedule deals with amendments to the India Evidence Act. It pertains to the inclusion of electronic document in the definition of evidence.
- The third schedule amends the Banker's Books Evidence Act. This amendment brings about change in the definition of "Banker's-book". It includes printouts of data stored in a floppy, disc, tape or any other form of electromagnetic data storage device. Similar change has been brought about in the expression "Certified-copy" to include such printouts within its purview.
- The fourth schedule amends the Reserve Bank of India Act. It pertains to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institution.

A major amendment was made in 2008. Amendment introduced the Section 66A which penalized sending of "offensive messages". It also introduced the Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". It also introduced penalties for child porn, cyber terrorism and voyeurism. Amendment was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed by the then President (Pratibha Patil) on 5 February 2009.

Objectives of the Amendments in The Information Technology Act, 2000

- With proliferation of information technology enabled services such as e-governance, 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.
- A rapid increase in the use of computer and internet has given rise to new forms of crimeslike publishing sexually explicit materials in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation 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.
- The United Nations Commission on International Trade Law (UNCITRAL) in the year 2001 adopted the Model Law on Electronic Signatures. The General Assembly of 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.
- 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.

Offences under The Information Technology Act, 2000

The Information Technology Act, 2000 has specified that Tampering with computer source documents, Hacking computer system, Publishing of information which is obscene in electronic form or failure of a CA or its employees to follow the directions/ Orders of the CCA, failure to comply with Directions of Controller to a subscriber to extend facilities to decrypt information, accessing a protected system without proper authorization, material mis-representation, Penalty for publishing Electronic Signature Certificate false particulars, Publication for fraudulent purpose, sending of grossly offensive information, false information, etc., will be offences.
The various offences and corresponding punishments thus summarized and tabulated below with detailed explanation in the following:

Section	Offence	Description	Penalty
65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes	Imprisonment up to three years, or/and with fine up

		another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	to ₹200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000
66A	Publishing offensive, false or threatening information	Any person who sends by any means of a computer resource any information that is grossly offensive or has a menacing character; or any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult shall be punishable with imprisonment for a term which may extend to three years and with fine.	Imprisonment up to three years, with fine.
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fradulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	If a person captures, transmits or	Imprisonment up to

		publishes images of a person's private parts without his/her consent or knowledge.	three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminant into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child thus defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.

68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to three years, or/and with fine up to ₹200,000
69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.

71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to three years, or/and with fine up to ₹100,000