Indian IT ACT

The Information Technology Act, 2000 or ITA, 2000 or IT Act, was notified on October 17, 2000. It is the law that deals with cybercrime and electronic commerce in India. In this article, we will look at the objectives and features of the Information Technology Act, 2000.

Information Technology Act, 2000

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce (e-commerce) to bring uniformity in the law in different countries.

Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. **India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000**.

While the first draft was created by the Ministry of Commerce, Government of India as the ECommerce Act, 1998, it was redrafted as the 'Information Technology Bill, 1999', and passed in May 2000.

- **Objectives of the Act**

The Information Technology Act, 2000 provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.

This also involves the use of alternatives to a paper-based method of communication and information storage to facilitate the electronic filing of documents with the Government agencies.

Further, this act amended the Indian Penal Code 1860, the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891, and the Reserve Bank of India Act 1934. The objectives of the Act are as follows:

- Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.
- Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication
- Facilitate the electronic filing of documents with Government agencies and also departments
- Facilitate the electronic storage of data
- Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions
- Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

- **Features of the Information Technology Act, 2000**

All electronic contracts made through secure electronic channels are legally valid.

Legal recognition for digital signatures.

Security measures for electronic records and also digital signatures are in place

A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized

Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.

An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court

Digital Signatures will use an asymmetric cryptosystem and also a hash function

Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.

The Act applies to offences or contraventions committed outside India

Senior police officers and other officers can enter any public place and search and arrest without warrant

Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

- **Applicability and Non-Applicability of the Act**

Applicability

According to Section 1 (2), the Act extends to the entire country, which also includes Jammu and Kashmir. In order to include Jammu and Kashmir, the Act uses Article 253 of the constitution. Further, it does not take citizenship into account and provides extra-territorial jurisdiction.

Section 1 (2) along with Section 75, specifies that the Act is applicable to any offence or contravention committed outside India as well. If the conduct of person constituting the offence involves a computer or a computerized system or network located in India, then irrespective of his/her nationality, the person is punishable under the Act.

Lack of international cooperation is the only limitation of this provision.

Non-Applicability

According to Section 1 (4) of the Information Technology Act, 2000, the Act is not applicable to the following documents:

Execution of Negotiable Instrument under Negotiable Instruments Act, 1881, except cheques.

Execution of a Power of Attorney under the Powers of Attorney Act, 1882.

Creation of Trust under the Indian Trust Act, 1882.

Execution of a Will under the Indian Succession Act, 1925 including any other testamentary disposition

by whatever name called.

Entering into a contract for the sale of conveyance of immovable property or any interest in such property.

Any such class of documents or transactions as may be notified by the Central Government in the Gazette.

The primary objectives of the IT Act, 2000 are:

- Granting legal recognition to all transactions done through electronic data exchange, other means of electronic communication or e-commerce in place of the earlier paper-based communication.
- Providing legal recognition to digital signatures for the authentication of any information or matters requiring authentication.
- Facilitating the electronic filing of documents with different Government departments and also agencies.
- Facilitating the electronic storage of data
- Providing legal sanction and also facilitating the electronic transfer of funds between banks and financial institutions.
- Granting legal recognition to bankers for keeping the books of accounts in an electronic form. Further, this is granted under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

- **Cyber Laws of India**

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

We can categorize Cyber crimes in two ways

The Computer as a Target :-using a computer to attack other computers.

e.g. Hacking,Virus/Worm attacks,DOS attack etc.

The computer as a weapon :-using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations,Credit card frauds,EFT frauds, Pornography etc.

Cyber law (also referred to as cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

Cyber Law in INDIA, Why Cyberlaw in India ?

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

What is the importance of Cyberlaw ?

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

Does Cyber law concern me ?

Yes, Cyberlaw does concern you. As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyberlegal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails , to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyberlaw issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyberlaw for your own benefit.

Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

Digital signatures have been given legal validity and sanction in the Act.

The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

The Act now allows Government to issue notification on the web thus heralding e-governance.

The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

Salient Features of I.T Act

- The salient features of the I.T Act 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.
- It 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.
- It 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.

Scheme of I.T Act

The following points define the scheme of the I.T. Act −

The I.T. Act contains 13 chapters and 90 sections.

The last four sections namely sections 91 to 94 in the I.T. Act 2000 deals with the amendments to the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934 were deleted.

It commences with Preliminary aspect in Chapter 1, which deals with the short, title, extent, commencement and application of the Act in Section 1. Section 2 provides Definition.

Chapter 2 deals with the authentication of electronic records, digital signatures, electronic signatures, etc.

Chapter 11 deals with offences and penalties. A series of offences have been provided along with punishment in this part of The Act.

Thereafter the provisions about due diligence, role of intermediaries and some miscellaneous provisions are been stated.

The Act is embedded with two schedules. The First Schedule deals with Documents or Transactions to which the Act shall not apply. The Second Schedule deals with electronic signature or electronic authentication technique and procedure. The Third and Fourth Schedule are omitted.

Application of the I.T Act

As per the sub clause (4) of Section 1, nothing in this Act shall apply to documents or transactions specified in First Schedule. Following are the documents or transactions to which the Act shall not apply −

Negotiable Instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;

A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;

A trust as defined in section 3 of the Indian Trusts Act, 1882;

A will as defined in clause (h) of section 2 of 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 may be notified by the Central Government.

Amendments Brought in the I.T Act

The I.T. Act 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.

Intermediary Liability

Intermediary, dealing with any specific electronic records, is a person who on behalf of another person accepts, stores or transmits that record or provides any service with respect to that record.

According to the above mentioned definition, it includes the following −

- Telecom service providers
- Network service providers
- Internet service providers
- Web-hosting service providers
- Search engines
- Online payment sites
- Online auction sites
- Online market places and cyber cafes
- Highlights of the Amended Act

The newly amended act came with following highlights −

- It stresses on privacy issues and highlights information security.
- It elaborates Digital Signature.
- It clarifies rational security practices for corporate.
- It focuses on the role of Intermediaries.
- New faces of Cyber Crime were added.

The Information Technology (Amendment) Act, 2008

The main Indian act that addresses legal challenges specifically as they relate to the Internet is the Information Technology (Amendment) Act, 2008, or for short, the IT Act. We highlight the sections that have the greatest relevance for the Internet and democracy.

- **Section 69A and the Blocking Rules: Allowing the Government to block content under certain circumstances**

Section 69A of the IT (Amendment) Act, 2008, allows the Central Government to block content where it believes that this content threatens the security of the State; the sovereignty, integrity or defence of India; friendly relations with foreign States; public order; or to prevent incitement for the commission of a cognisable offence relating to any of the above. A set of procedures and safeguards to which the Government has to adhere when doing so have been laid down in what have become known as the Blocking Rules.

- **Section 79 and the IT Rules: Privatising censorship in India**

Section 79 of the Information Technology (Amendment) Act, 2008 regulates the liability of a wide range of intermediaries in India. The section came in the limelight mostly because of the infamous Intermediary Guidelines Rules, or IT Rules, which were made under it. The IT Rules constitute an important and worrying move towards the privatisation of censorship in India.

- **Sections 67 and 67A: No nudity, please**

The large amounts of 'obscene' material that circulate on the Internet have long attracted comment in India. Not surprsingly, then, in the same way as obscenity is prohobited offline in the country, so it is online as well. The most important tools to curtail it are sections 67 and 67A of the IT Act, prohibiting obscene and sexually explicit material respectively.

- **Section 66A: Do not send offensive messages**

Section 66A of the Information Technology (Amendment) Act, 2008 prohibits the sending of offensive messages though a communication device (i.e. through an online medium). The types of information this covers are offensive messages of a menacing character, or a message that the sender knows to be false but is sent for the purpose of 'causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will.' If you're booked under Section 66A, you could face up to 3 years of imprisonment along with a fine.