MODULE -5

Introduction to IT ACT 2000

The Government of India enacted The Information Technology Act with some major objectives which are as follows −

- To deliver lawful recognition for transactions through electronic data interchange (EDI) and other means of electronic communication, commonly referred to as **electronic commerce** or E-Commerce. The aim was to use replacements of 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 Bankers' 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, was thus passed as the Act No.21 of 2000. The I. T. Act got the President’s assent on June 9, 2000 and it was made effective from October 17, 2000. By adopting this Cyber Legislation, India became the 12th nation in the world to adopt a Cyber Law regime.

SALIENT FEATURES OF IT 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.

Amendment of IT ACT 2000

- The IT **Amendment Act** was passed by the Indian Parliament in October **2008** and came into force a year later. ...
  The **Amendment** was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original **law** was passed

- **Data Protection**
  The IT Act 2000 did not have any specific reference to Data Protection, the closet being a provision to treat data vandalism as an offense. The Government introduced a separate bill called "Personal Data Protection Act 2006," which is pending in the Parliament and is likely to lapse.
- The IT(A) Act 2008 has introduced two sections that address data protection aspects.

- **The sections under consideration are:**
- Section 43A: Compensation for failure to protect data
- Section 72A: Punishment for disclosure of information in breach of lawful contract

DESCRIPTION OF SECTION 43

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected.

- By way of explanation: “Body corporate means Indian companies”.
- “Reasonable security practices mean a mutual contract between the customer and service provider OR as per the specified law. In the absence of both then as specified by the Central Government.
- Hence it would be important for Indian companies to seriously look at SLAs and agreements which have been signed with clients to understand the data protection implications. The same goes for understanding the applicable laws.
- A major modification is that this clause doesn’t mention the compensation limit of Rs. 1 Crore, which was there as part of section 43 of the IT Act 2000. This implies that there is no upper limit for damages that can be claimed. This essentially is “unlimited liability” for Indian companies, which could cause serious business

Information Security

Across the amendments there are several references to “service providers” or “intermediaries”, which in some form would apply to all Indian companies.

- **Example - Section 67C**
  Preservation and retention of information by intermediaries. Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe”.
- Any intermediary who intentionally or knowingly contravenes the provisions shall be punished with an imprisonment for a term which may extend to 3 years and shall also be liable to fine.
- The notifications on time for preservation etc. are not yet released. However, since this is a “cognizable” offense any police inspector can start investigations against the CEO of a company.

- Apart from the two aspects discussed in this note, there are other areas which could also be considered.
- **Sec 69:** Power to issue directions for interception or monitoring or decryption of any information through any computer resource.
- **Sec 69B:** Power to authorize to monitor and collect traffic data or information through any computer resource for cybersecurity, etc..

Cyber risk management and response must be revisited by every enterprise to secure critical assets and meet compliance needs. The IT(A) act 2008 amendments provide a few additional factors that can have a significant impact on business. Information technology regulations and laws are sure to get more stringent and defined, making organizations more prepared to take on today's threats.

Cyberspace

Cyberspace can be defined as **an intricate environment that involves interactions between people, software, and services**. It is maintained by the worldwide distribution of information and communication technology devices and networks.

Right to privacy means

- Right to be alone
- It is a human right and has been recognized in Article 8 of European Convention on Human Rights 1950 .

Violation of the right of privacy in Cyberspace/Internet punishments for violation of privacy

- Violation of privacy: Section 66E of the IT Act prescribes punishment for violation of privacy and provides that any person who intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person

The above Section punishes intentionally or knowingly capturing, publishing or transmitting the image of a private area without the consent of that person which violates the privacy of that person is punishable with imprisonment up to three years or with fine up to two lakh rupees or with both imprisonment and fine. The Section requires *mens rea* on the part of the offender in the form of either intention or knowledge of violating privacy of a person. The offence is also cognizable as well as bailable under Section 77B of the IT Act.

The above offence defined provides for meaning to various situations under the explanation which are as follows:

(a) 'transmit' means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) 'capture', with respect to an image, means to videotape, photograph, film or record by any means;

(c) 'private area' means the naked or undergarments clad genitals, public area, buttocks or female breast;

(d) 'publishes' means reproduction in the printed or electronic form and making it available for public;

(e) 'under circumstances violating privacy' means circumstances in which a person can have a reasonable expectation that—

  (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

  (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

- Sometimes many websites use web bugs to tracks as to who is viewing there pages. The web bug can confirm when the message or web page and record the IP address of the viewer.
- Sometimes direct marketing online newspapers and other businesses have friendly boxes asking for if the websites can save our account information for future transactions.
- Even spyware are software that secretly gather the information through our Internet connection without our knowledge.
- Lastly, phishing and pharming that deceive us into revealing our personal information.

On cyberspace, with the use of Internet, we provide information to others in many ways. Even though the information we provide to one person or company on the Internet may not make sense unless it is combined with information we provide to another person or company. Some of the methods by which we provide information to others are as follows:

- When we sign with an Internet Service Providers (ISP). The ISP provides mechanism for connecting the computer to the Internet. Each computer connected to the Internet has a unique address known as the IP address.
- When we correspond through e-mail we are giving information to the recipient. By e-mail we might also be giving information to our employer, the government, our e-mail provider and to anyone that the recipient of e-mail passes our message to.
- By browsing through Internet we are also relying personal information to websites.
- When we use search engines on Internet the search engines also have the availability to track our searches.
- The instant messaging/chatting/video conferencing in all these methods can be archived, stored and recorded on our computer as easily as e-mails, which can also affect privacy.
- Blogging where people post a video or photograph online also can affect privacy.
- Even online banking requires a lot of sensitive information over the internet, which may affect privacy.

- Sometimes many websites use web bugs to tracks as to who is viewing there pages. The web bug can confirm when the message or web page and record the IP address of the viewer.
- Sometimes direct marketing online newspapers and other businesses have friendly boxes asking for if the websites can save our account information for future transactions.
- Even spyware are software that secretly gather the information through our Internet connection without our knowledge.
- Lastly, phishing and pharming that deceive us into revealing our personal information.

PHISHING AND PHARMING

- Phishing is a technique used by hackers to acquire your personal information by sending an email that is designed to look just like a legitimate email and is intended to trick you into clicking on a malicious link or attachment.
- Unfortunately, emails are not the only way phishers try to trick you, they can also send texts (SMiShing), use voice messages (Vishing), and even send faxes (Phaxing) in their efforts to gain access to your sensitive information.
- It's extremely important to know how to protect yourself from a phishing scam, as phishing accounts for 91% of all incidents. In order to protect yourself and your organization from phishing attacks follow these tips:
- Make sure your operating system and your antivirus software are up-to-date
- Hover over links in emails and on websites to verify the destination
- Try typing in the website's address rather than clicking a link from an email message
- Always be cautious of sensational subject lines and language, like "Must Act Now!" or contain spelling and grammar errors.
- If an email simply looks suspicious, it's best to delete it

- Pharming is the fraudulent practice of redirecting the users to a fake website that mimics the appearance of a legitimate one, with the goal of stealing personal information such as passwords, account numbers, and other personal information.
- Pharming can occur even when you click an authentic link or type in the website URL yourself because the website's domain name system (DNS) has been hijacked by a cyber-criminal. Like a phishing attack, pharming is dangerous because it's difficult to recognize the dangers lurking on the site causing many users to unknowingly hand over their personal information to the hackers.
- So, how can you protect yourself against such a sneaky cyber-crime? Before transmitting sensitive information on a website, be sure to remember the following tips:
- Install reliable security software or make sure your current software and system are up to date
- Make sure the site is on a HTTPS server
- Look for the padlock in the corner of the screen
- Check if the website is certified by an Internet Trust Organization
- Check the website's certificate and encryption levels
- Access the website through its specific IP address rather than web name
- Although you may feel confident about defending yourself from a phishing or pharming attack, an organization is only as safe as its weakest link. Let the experts at Inspired eLearning put your employees through cybersecurity training and phishing awareness training to keep your business safe and secure.
-

Some of the examples of phishing are a banking fraud. Here the hackers try to get your bank details by acting as a bank employee. They communicate and steal the information in a fraudulent way.

BREACH OF CONFIDENTIALITY AND PRIVACY

Breach of privacy and Confidentiality under information Technology Act, 2000. Privacy as a concept involves what privacy entails and how it is to be valued. ... In the legal parlance the issue of confidentiality comes up where an obligation of confidence arises between a 'data collector and a 'data subject.

Under the above Section, breach of confidentiality and privacy when a person discloses such electronic records to other persons who are not authorised to get such information about documents and records, is punishable with imprisonment up to two years or with a fine which may extend to one lakh rupees, or with both. As the offence under Section 72 of the IT Act is punishable for maximum imprisonment of only two years, therefore, the offence under this section is non-cognizable under section 77B of this Act. Moreover, the offence is bailable under section 77B. As the offence can be committed by disclosure to any other person without the consent of that person who is authorised to give such consent, it appears that the offence under this section requires positive disclosure on the part of the offender in order to commit the offence under this Section.

The above Section 72 relating to confidentiality and privacy must be understood along with the reasonable restrictions provided under Article 19(2) viz; reasonable restrictions on the right of freedom of speech and expression in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

With the amendment of the IT (Amendment) Act, 2008, a new Section 72A has been introduced where by any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any person, shall be punished with imprisonment for a

Term which may extend upto five years or five lakhs punishment or both.

Section 77B of the Act states that notwithstanding anything contained in the Code of Criminal Procedure, 1973 the **offence punishable with imprisonment of three years and above shall be cognizable** and the offence punishable with imprisonment of three years shall be bailable

CYBER TERRORISM

- Is a combination of cyberspace+terrorism
- Cyberterrorism is the convergence of cyberspace and terrorism. It refers to **unlawful attacks and threats of attacks against computers, networks** and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.
- In order to properly called cyber terrorism attacks should be result into violence against persons,property or society resulting in extreme harm and high fear among people.

Cyber terrorism has special features to make a distinction between a cyber terror attack and the activities of a hacker. The cyber terrorist attack is pre-defined and the victims are generally specific targets and the cyber terrorist's attacks objective is to destroy or damage specific targets like political, civil, economic, energy and military infrastructure. And the object is to cause fear in order to achieve their political, religious or economic goals. They persuade people to believe that the victims are vulnerable and their machinery negligent.

INTER MEDIARIES

An Intermediary is an Internet Service Provider which provides its platform for selling any goods or services or providing any service relating to an electronic record or communication. It would include any web hosting company, online auction site, online market place, or online payment sites and cybercafes. It includes network and telecom service providers too. Thus, it would include carriers of information (such as gmail service) and also a payment gateway (such as Pay pal, or Pay tm service)

Under Information Technology Act, 2000, Section 2(1) (w) defines an ‘Intermediary’ as ‘any person who on behalf of another person receives, stores, transmits that record or provides any service with respect to electronic record and 2 liability of Intermediaries includes telecom service providers, internet service providers, web hosting service providers, search engines, online payment sites, online auction sites, online market place and cyber café.

LIABILITIES OF INTERMEDIARIES

- In India,Section 79 of the Information Technology Act, 2000 specifically deals with the issue of liability of Intermediaries.
- It states that an Intermediary is not liable for any third party information, data or communication link made available or hosted by him except as specified in Sections 79(2) and (3) of the IT Act,2000.

  The 'third party information' is described in explanation 2 to Section 79 of the IT Act,2000 as any information dealt with by an Intermediary in his position as an Intermediary. For example, a social media portal is an intermediary where users may post third party information by posting the user generated content such as pictures, comments or other posts.

  According to Section 79(2) of the IT Act,2000, an Intermediary is not liable if its only role is to provide access to a communication system over, which information is posted by third party and 'transmitted or temporarily stored or hosted'.

Further, the section provides that an Intermediary is not liable if it neither initiates the transmissions nor selects recipients and select 4 liability of Intermediaries or change the information contained in the message which is transmitted.

An Intermediary is liable not for third party information if it complies with due diligence requirements laid down by the Central Government.

Section 79(3) of the IT Act,2000 prescribes the conditions when an Intermediary is liable for third party information. An Intermediary is liable for third-party information, if it conspires or abets or aids or induces through threats or promises or otherwise to commit an unlawful act.

The Intermediary is liable if on receiving actual knowledge or receiving a notice from the Government or its Agency that any information residing in or connected to a computer resource which is managed by an Intermediary used to commit an illegal act and the Intermediary thereafter does not efficaciously remove that material without tampering or destroying the evidence in any manner.

Offences by Intermediaries

Under Section 67C of IT (Amendment) Act, 2008—

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

The above Section requires the intermediary to preserve and retain information for such duration and format as the Central Government may prescribe. Any violation by the intermediary who intentionally or knowingly contravenes the provisions under this Section shall be punished for an imprisonment up to three years and also shall be liable to fine. The above mentioned offence requires *mens rea* on the part of the intermediary to commit an offence. The offence is also cognizable and bailable under Section 77B of the Act.

(a) Exemption from Liability of Intermediary in Certain Cases.

Under Chapter XII of the IT (Amendment) Act, 2008, Section 79 states—

(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) intermediary does not—

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if—

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promises or authorises in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate government or its agency that any information, data or communication link residing in or connected to a computer resource, controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Offences Relating to Protected System

Section 70 as amended by the IT (Amendment) Act, 2008 provides—

(1) The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.
Explanation: For the purposes of this section, 'Critical Information Infrastructure' means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.

(2) The appropriate government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

practices and procedures for such protected system.

The above Section provides for the offence relating to protected system which directly or indirectly affects the Critical Information Infrastructure. The object of the offence is to prevent the incapacitation or destruction of computer resource which may have debilitating impact on national security, economy, public health

or safety. The appropriate Government may by order in writing, authorise the persons who are authorised to access protected system. The contravention of the provisions of this section is serious offence which may be punished with imprisonment up to ten years and shall also be liable to fine. The offence is cognizable and also non-bailable under Section 77B of the Act.

Section 71. Penalty for misrepresentation:

(1) Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Penalties: Punishment: imprisonment which may extend to two years
Fine: may extend to one lakh rupees or with both.

Punishment to Abetment and Attempt to Commit Offences under the IT Act

84B. Punishment for abetment of offences. - Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act.

Explanation.-An act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.]

Under Section 84C of the IT (Amendment) Act, 2008, any person who attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment

of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.