



Session 2-Explain compliance with IT Act

Session2-Explain compliance with IT Act

Identify What is Considered as a Cyber Crime as per IT Act – Cyber Crime

- In this world, where everything is available at a click, crimes are also been committed at a click. Cyber Crime thus is the darker side of technology. It is a Crime where the computer is either a tool or a target.
- Therefore, it stands to reason that "cyber-crimes" are offences relating to computers, information technology, internet and virtual reality

Information Technology Act 2000

- Computer network Section 2(a) and 2(j) Information Types
- Computer Section 2(i)
- Data Section 2(o)
- Information Section 2(v)

These are all the necessary ingredients that are useful to technically understand the concept of Cyber Crime.

The Preamble of the IT Act

Objective 1

- 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 commerce", which involve the use of alternatives to paper-based methods of communication and storage of information

Objective 2

- 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."

Silent features of the Act are

- The Act gives legal recognition of Electronic Documents.
- The Act gives legal recognition of Digital Signatures.
- It describes and elaborates Offenses, penalties and Contraventions.
- It gives outline of the Justice Dispensation Systems for cyber crimes.
- The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act.

Cyber Crime as per IT Act

Scheme of the IT Act

- The IT Act is spread in total 13 chapters.
- There are total 90 sections, the last four sections namely sections 91 to 94 in the I. T. Act 2000 dealt 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.

Definitions in the IT Act

Section 2(a)	Access	Section 2(r)	Electronic Form
Section 2(b)	Addressee	Section 2(s)	Electronic Gazette
Section 2(c)	Adjudicating Officer	Section 2(t)	Electronic Record
Section 2(d)	Affixing	Section 2(ta)	Electronic Signature
Section 2(e)	Appropriate Authority	Section 2(tb)	Electronic Signature Certificate
Section 2(f)	Asymmetric Crypto System	Section 2(u)	Function
Section 2(g)	Certifying Authority	Section 2(ua)	Indian Computer Emergency Response Team
Section 2(h)	Certification Practice Statement	Section 2(v)	Information
Section 2(ha)	Communication Device	Section 2(w)	Intermediary
Section 2(i)	Computer	Section 2(x)	Key Pair
Section 2(j)	Computer Network	Section 2(y)	Law
Section 2(k)	Computer Resource	Section 2(z)	Licence
Section 2(l)	Computer System	Section 2(za)	Originator
Section 2(m)	Controller	Section 2(zb)	Prescribed
Section 2(n)	Cyber Appellate Tribunal	Section 2(zc)	Private key
Section 2(na)	Cyber Café	Section 2(zd)	Public key
Section 2(nb)	Cyber Security	Section 2(ze)	Secure system
Section 2(o)	Data	Section 2(zf)	Security procedure
Section 2(p)	Digital Signature	Section 2(zg)	Subscriber
Section 2(q)	Digital Signature Certificate	Section 2(zh)	Verify

Privacy and Privacy Protection

Highlights of Amended Information Technology Act 2008

- It focuses on privacy issues.
- It focuses on Information Security.
- It came with surveillance on Cyber Cases.
- The Concept of Digital Signature was elaborated.
- It clarified reasonable security practices for corporate.
- Role of Intermediaries were focuses.
- It came with the Indian Computer Emergency Response Team.
- New faces of Cyber Crime were added.
- Powers were given to Inspector to investigate

IT Act 2000

- Section 3 of the Act provides for authentication of Electronic Records by affixing his Digital Signature.

- It shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Amended IT Act 2008

- By the Amendment Act of 2008 Section 3(A) was embedded in the Act. The newly added provision provides for authentication of electronic record by electronic signature or electronic authentication technique which is, considered reliable and may be specified in the second schedule.
- Sub Clause (2) provides the circumstances in which the electronic signature or electronic authentication technique shall be considered reliable.

Cyber Crime as per IT Act

Digital Signature to Electronic Signature

According to the UNCITRAL MODEL LAW on Electronic Signatures, technologies currently in use for electronic signature includes:

- Digital Signature within a public key infrastructure (PKI)
- Biometric Device
- PINs
- Passwords
- Scanned handwritten signature
- Signature by Digital Pen

- Clickable "OK" or "I Accept" or "I Agree" click boxes

Identify the Penalties for Cyber Crimes

Here are a few examples of cyber-crimes penalised by the IPC and the IT Act.

- Hacking and Data Theft
- Receipt of stolen property
- Identity theft and cheating by personation
- Obscenity

Receipt of stolen property

- **Section 66B of the IT Act** prescribes punishment for dishonestly receiving any stolen computer resource or communication device. This section requires that the person receiving the stolen property ought to have done so dishonestly or should have reason to believe that it was stolen property. The punishment for this offence under Section 66B of the IT Act is imprisonment of up to 3 (three) years or a fine of up to Rs. 1,00,000 (Rupees one lac) or both.

Identity theft and cheating by personation

- **Section 66C of the IT Act** prescribes punishment for identity theft and provides that anyone who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).
- **Section 66D of the IT Act** prescribes punishment for 'cheating by personation by using computer resource' and provides that any person who by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).
- **Section 419 of the IPC** also prescribes punishment for 'cheating by personation' and provides that any person who cheats by personation shall be punished with imprisonment of either **description for a term which may extend to 3 (three) years or with a fine or with both.**
- **Section 468 of the IPC** prescribes punishment for forgery for the purpose of cheating and provides a punishment of imprisonment of either description for a term which may extend to 7 (seven) years and also a fine.
- **Section 420 of the IPC** that provides that any person who cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security shall be punished with imprisonment of either description for a term which may extend to 7 (seven) years, and shall also be liable to fine.

Obscenity

- **Sections 67, 67A and 67B of the IT Act** prescribe punishment for publishing or transmitting, in electronic form: (i) obscene material; (ii) material containing sexually explicit act, etc.; and (iii) material depicting children in sexually explicit act, etc. respectively.
- The punishment prescribed for an offence under section 67 of the IT Act is, on the first conviction, imprisonment of either description for a term which may extend to 3 (three) years, to be accompanied by a fine which may extend to Rs. 5,00,000 (Rupees five lac), and in the event of a second or subsequent conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac).
- The punishment prescribed for offences under sections 67A and 67B of the IT Act is on first conviction, imprisonment of either description for a term which may extend to 5 (five) years, to be accompanied by a fine which may extend to Rs. 10,00,000 (Rupees ten lac) and in the event of second or subsequent conviction, imprisonment of either description for a term which may extend to 7 (seven) years and also with fine which may extend to Rs. 10,00,000 (Rupees ten lac).

Cyber-crimes penalized by the IT Act that do not have an equivalent in the IPC

1. Section 43(h) of the IT Act

- Section 43(h) read with section 66 of the IT Act penalises an individual who charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network. A person who tampers with the computer system of an electricity supplier and causes his neighbour to pay for his electricity consumption would fall under the aforesaid section 43(h) of the IT Act for which there is no equivalent provision in the IPC.

2. Section 65 of the IT Act

- Section 65 of the IT Act prescribes punishment for tampering with computer source documents and provides that any person who knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code (i.e. a listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form) 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, shall be punishable with imprisonment for up to 3 (three) years or with a fine which may extend to Rs. 3,00,000 (Rupees lac) or with both.
- To a certain extent, section 409 of the IPC overlaps with section 65 of the IT Act. Section 409 of the IPC

provides that any person who is in any manner entrusted with property, or with any dominion over property in his capacity as a public servant or in the way of his business as a banker, merchant, factor, broker, attorney or agent, commits criminal breach of trust in respect of that property, shall be punished with imprisonment for life or with imprisonment of either description for a term which may extend to 10 (ten) years, and shall also be liable to a fine. However, section 65 of the IT Act does not require that the person who tampers with or damages or destroys computer source documents should have been entrusted with such source code. Under section 409 of the IPC, criminal breach of trust should have been committed by someone to whom the property was entrusted.

3. 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, shall be punished with imprisonment which may extend to 3 (three) years or with fine not exceeding Rs. 2,00,000 (Rupees two lac) or with both.
- There is no provision in the IPC that mirrors Section 66E of the IT Act, though sections 292 and 509 of the IPC do cover this offence partially.
- Section 509 of the IPC provides that if any person intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, such person shall be punished with simple imprisonment for a term which may extend to 1 (one) year, or with fine, or with both. Unlike section 66E of the IT Act which applies to victims of both genders, section 509 of the IPC applies only if the victim is a woman.

4. Section 67C of the IT Act

Section 67C of the IT Act requires an 'intermediary' to preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. The section further provides that any intermediary who intentionally or knowingly contravenes this requirement shall be punished with imprisonment for a term which may extend to 3 (three) years and also be liable to a fine.

5. Cyber terrorism

- Section 66F of the IT Act prescribes punishment for cyber terrorism. Whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people, denies or causes the denial of access to any person authorized to access a computer resource, or attempts to penetrate or access a computer resource without authorisation or exceeding authorised access, or introduces or causes the introduction of any computer contaminant, and by

means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect critical information infrastructure, is guilty of 'cyber terrorism'.

- Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.
- There is no provision in the IPC that mirrors section 66F of the IT Act, though section 121 of the IPC (waging, or attempting to wage war, or abetting waging of war, against the Government of India) does cover this offence partially.

6. Section 77A of the IT Act

Section 77A of the IT Act provides that, subject to certain exceptions, all offences under the IT Act for which the punishment is imprisonment for a term of 3 (three) years or less, are compoundable. The provisions of sections 265B and 265C of the Code of Criminal Procedure, 1973 ("CrPC") shall apply with respect to such compounding.

7. Section 77B of the IT Act

Section 77B of the IT Act provides that notwithstanding anything contained in the CrPC, all offences punishable with imprisonment of 3 (three) years and above under the IT Act shall be cognizable and all offences punishable with imprisonment of 3 (three) years or less shall be bailable.

Cyber-crimes covered under the IT Act are punishable with imprisonment of 3 (three) years or less.

- The cyber-crimes which are punishable with imprisonment of more than 3 (three) years are:
- Publishing or transmitting obscene material in electronic form under section 67 of the IT Act
- Publishing or transmitting of material containing sexually explicit act, etc., in electronic form under section 67A of the IT Act
- Publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form under section 67B of the IT Act
- Cyber terrorism under section 66F of the IT Act

Conflict between the IPC and the IT Act: Case Law

The overlap between the provisions of the IPC and the IT Act may sometimes lead to an anomalous situation wherein certain offences are bailable under the IPC and not under the IT Act and vice versa and certain offences are compoundable under the IPC and not under the IT Act and vice versa.

IPC's Treatment of Stalking

The legislature's treatment of the offence of "stalking", accomplished through the insertion of new section 354D in the IPC through the Criminal Law (Amendment) Act, 2013⁵, is a case in point.

- Section 354D penalises the offence of "stalking" whether it has a cyber component or not.
- If a man follows a woman and contacts, or attempts to contact, such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman, it amounts to stalking.
- If a man monitors the use by a woman of the internet, email or any other form of electronic communication, it will also result in the offence of stalking. There are a few exemptions to this offence of stalking, and all the defences apply irrespective of whether the stalking is cyber stalking or not.
- The punishment prescribed for stalking by Section 354D of the IPC does not discriminate on the basis of the presence or absence of the "cyber" component.

Amendments to the IPC to Cover Cyber-crimes

- A new section 29A was created to define "electronic record" by linking it with the definition given in the IT Act⁶.
- A new sub-section (3) was inserted in section 4 of the IPC that states that the provisions of the IPC shall be applicable to any person in any place "without and beyond India", committing an offence targeting a computer resource located in India.
- In sections 118 and 119 of the IPC the words "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design" were inserted before the words "to commit such offence or makes any representation which he knows to be false respecting such design".
- In section 464 of the IPC (which penalises the making of a false document), the phrase "digital signature" was replaced with the phrase "electronic signature" in all places.
- "Electronic record" was included within the ambit of sections 164, 172, 173, 175, 192, 204, 463, 466, 468, 469, 470, 471, 474 and 476 of the IPC that earlier only provided for "documents", "books", "paper", "writing" or "records".
- In section 466 of the IPC, the term "register" was defined to include any list, data or record of any entries maintained in an "electronic form", as defined in section 2(1) (r) of the IT Act¹⁰.
- A new section 354D was inserted in the IPC that introduces the offence of cyber stalking

Recap:

- Cyber-crimes are offences related to computers, information technology, internet and virtual reality
- The Information Technology Act, 2000 ("IT Act") and the Indian Penal Code, 1860 ("IPC") penalise a number of cyber-crimes and unsurprisingly, there are many provisions in the IPC and the IT Act that overlap with each other.
- Most of the cyber-crimes covered under the IT Act are punishable with imprisonment of 3 (three) years or less.
- The punishment prescribed for stalking by Section 354D of the IPC does not discriminate on the basis of the presence or absence of the "cyber" component.

