Module 5
Part 1

Information Technology Act and Punishments

Index

- Introduction to IT Act 2000
- Amendments on IT Act
- Violation of the right of privacy in cyberspace/internet
- Punishment for violation of privacy, breach of confidentiality and privacy under IT act
- Terrorism on cyberspace

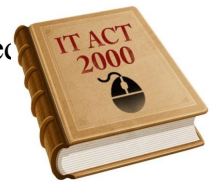
Information Technology Act, 2000

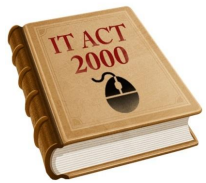
सत्यमेव जयते

Introduction to IT Act 2000

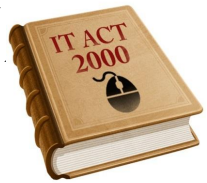
- The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000
- It is the primary law in India dealing with cybercrime and electronic commerce
- Secondary or subordinate legislation to the IT Act includes the Intermediary Guidelines Rules 2011 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Enacted by	Parliament of India
Enacted	9 June 2000
Assented to	9 June 2000
Signed	9 May 2000
Commenced	17 October 2000
Introduced by	Pramod Mahajan Minister of Communications and Information Technology
Amended by	
IT (Amendment) Act 2008	

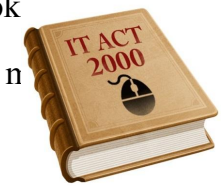




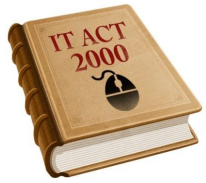
- The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 June 2000
- The bill was finalised by a group of officials headed by then Minister of Information Technology Pramod Mahajan
- The original Act contained 94 sections, divided into 13 chapters and 4 schedules
- The laws apply to the whole of India
- If a crime involves a computer or network located in India, persons of other nationalities can also be indicted under



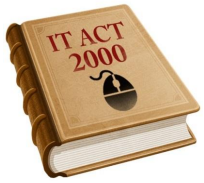
- The Act provides a legal framework for electronic governance by giving recognition to electronic records and digital signatures
- It also defines cyber crimes and prescribes penalties for them
- The Act directed the formation of a Controller of Certifying Authorities to regulate the issuance of digital signatures
- It also established a Cyber Appellate Tribunal to resolve disputes rising from this new law
- The Act also amended various sections of the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934 to make them compliant with new technologies



Section	Offence	Penalty
65	Tampering with computer source documents	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	Imprisonment up to three years, or/and with fine up to ₹100,000
66E	Publishing private images of others	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	Imprisonment up to seven years, or/and with fine up to ₹1,000,000



67B	Publishing child porn or predating children online	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	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	Imprisonment up to 2 years, or/and with fine up to ₹100,000
69	Failure/refusal to decrypt data	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	Imprisonment up to 2 years, or/and with fine up to ₹100,000
72	Breach of confidentiality and privacy	Imprisonment up to 2 years, or/and with fine up to ₹100,000
72A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years, or/and with fine up to ₹500,000
73	Publishing electronic signature certificate false in certain particulars	Imprisonment up to 2 years, or/and with fine up to ₹100,000
74	Publication for fraudulent purpose	Imprisonment up to 2 years, or/and with fine up to ₹100,000



❖ Amendments on IT Act

- A major amendment was made in 2008
- It introduced Section 66A which penalized sending "offensive messages“
- It also introduced Section 69, which gave authorities the power of "decryption of any information through any computer resource“
- Additionally, it introduced provisions addressing - pornography, child porn, cyber terrorism and voyeurism
- The 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 into law by President Pratibha Pati

THE AMENDMENTS

From its establishment as an amendment to the original act in 2008, Section 66A attracted controversy over its unconstitutional nature:

Section	Offence	Description
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.

- On 24 March 2015, the Supreme Court of India, gave the verdict that Section 66A is unconstitutional in entirety
- The court said that Section 66A of IT Act 2000 is "arbitrarily, excessively and disproportionately invades the right of free speech" provided under Article 19(1) of the Constitution of India
- But the Court turned down a plea to strike down sections 69A and 79 of the Act, which deal with the procedure and safeguards for blocking certain websites

THE AMENDMENTS

❖ Violation of the right of privacy in cyberspace/internet

- **Refer Textbook :** Harish Chander, “Cyber Law and IT Protection”, PHI Learning Pvt.Ltd.

❖ Punishment for violation of privacy, breach of confidentiality and privacy under IT act

- **Refer Textbook :** Harish Chander, “Cyber Law and IT Protection”, PHI Learning Pvt.Ltd.

❖ Terrorism on cyberspace

- Terrorism is a method to cause fear and undue violence against individuals, groups or countries and a big challenge in this world
- The causes of terrorism in this world are numerous including religious, geographical and against particular countries by one country against the other countries
- Terrorism is a complicated, complex and a very challenging task
- There is no unanimity among the people about the methods to regulate the phenomenon of terrorism in this wo

- The beginning of cyber terrorism can be traced right from early 1990s when the increase in the growth of Internet and cyberspace was visible in this world
- Cyber terrorist's attacks objectives :
  - Destroy or damage specific targets like political, civil, economic, energy and military infrastructure
  - To cause fear in order to achieve their political, religious or economic goals
  - They persuade people to believe that the victims are vulnerable
- In India with the amendment of IT (Amendment) new provision has been introduced for the punishm Terrorism which pr ides

- Terrorists also use Internet and cyberspace frequently in order to achieve their terrorists objectives
- The possibility of speedy, anonymous, accurate and timely information with the help of Internet and cyberspace gives competitive advantage to the terrorist and terrorists groups
- The expression 'cyber terrorism' in fact is a combination of the words cyberspace and terrorism
- Which means unlawful attacks and threats of attacks, against computer, networks and the information stored in the computer systems to intimidate the governments o social or reli ious objectives

(1) Whoever:

(a) 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 by—

(i) Denying or causing the denial of access to any person authorized to access computer resource; or

(ii) Attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) Introducing or causing to introduce 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 knows that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affects the critical information infrastructure specified under section 70; or

(b) Knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests 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, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

- **Section 66F**
- **Offence is cognizable and non-bailable according to section 77B of the IT Act**