

# Legal framework for Digital Forensics-II : IT Act 2000 with amendments

*E-Vimarsh: Lecture Notes for Digital Forensics Course*

*For M.Tech.(CSE) and Ph.D.(Coursework)*



**Prof Vikas Pareek**

**Head, Department of CS&IT**

**Mahatma Gandhi Central University, Bihar.**




# Index

- Introduction
- Information Technology Act 2000
- Salient features
- IT Act amendments
- Penalties for various Cyber crimes
- CERT-In Guidelines for Auditing and Logging
- Concluding Remarks
- References



# Information Technology Act 2000

- ▶ The Information Technology Act, 2000 ( 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.
- ▶ It is based on the UNCITRAL Model Law on International Commercial Arbitration recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.



- 
- ▶ 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 law.


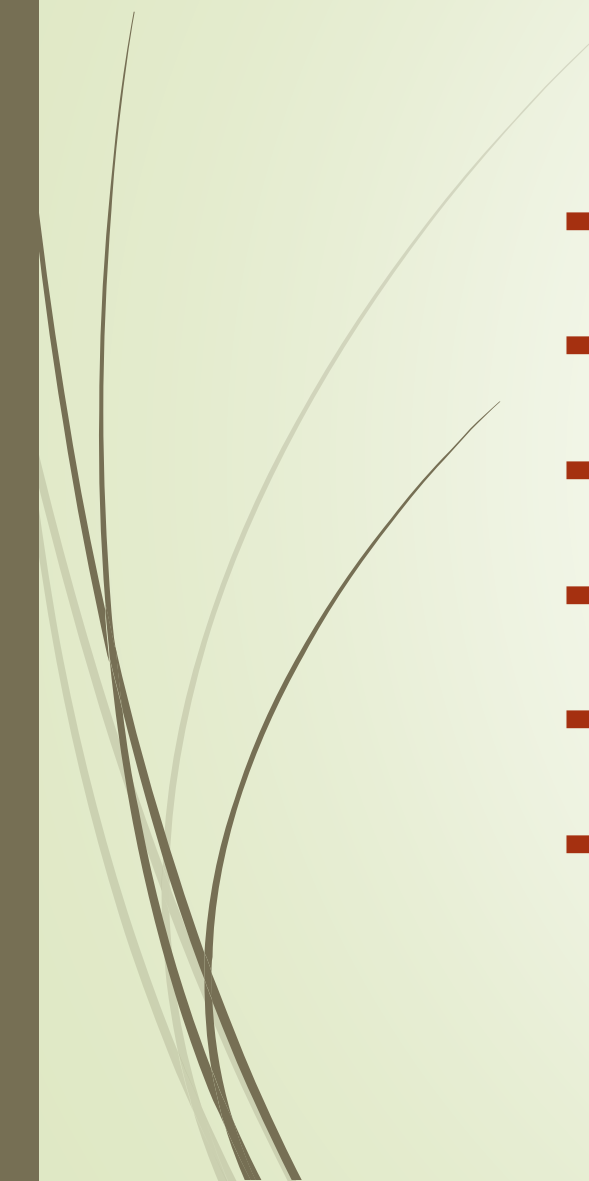


# Structure



- ▶ Chapter 1: Preliminary  
(this chapter covers section 1 to section 2)
- ▶ Chapter 2: Digital Signature and Electronic Signature  
(this chapter covers section 3 to section 3A)
- ▶ Chapter 3: Electronic Governance  
(this chapter covers section 4 to section 10A)
- ▶ Chapter 4: Attribution Acknowledgment and Dispatch of Electronic Records  
(this chapter covers section 11 to section 13)
- ▶

- 
- 
- ▶ Chapter 5: Secure Electronic Records And Secure Electronic Signatures  
(this chapter covers section 14 to section 16)
  - ▶ Chapter 6: Regulation of Certifying Authorities  
(this chapter covers section 17 to section 34)
  - ▶ Chapter 7: Electronic Signature Certificates  
(this chapter covers section 35 to section 39)
  - ▶ Chapter 8: Duties Of Subscribers  
(this chapter covers section 40 to section 42)


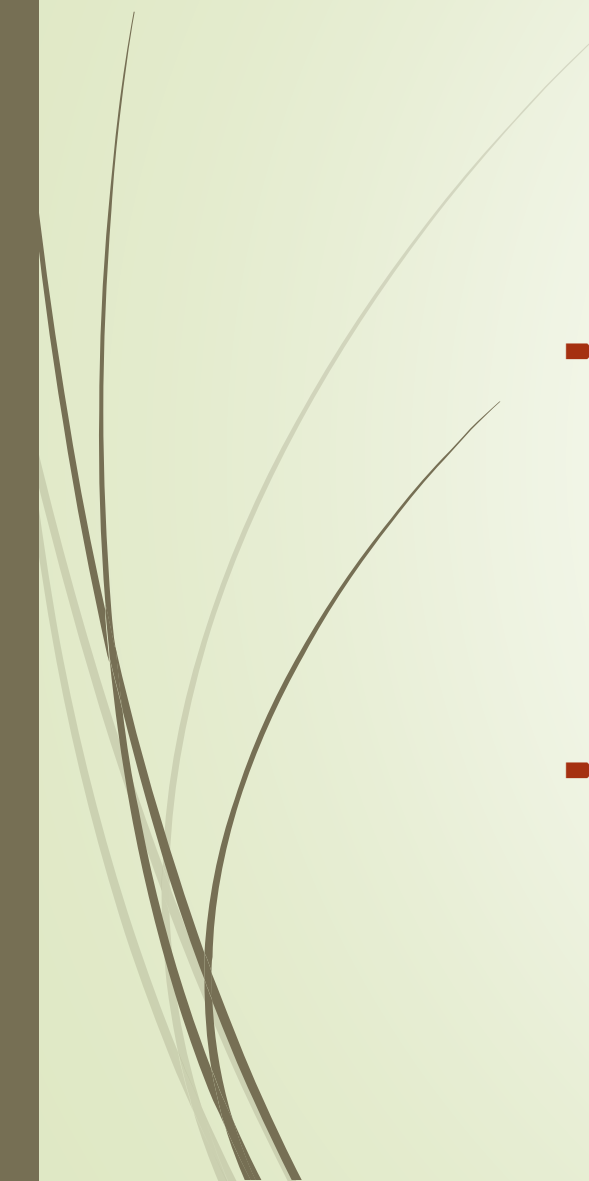
- 
- 
- ▶ Chapter 9: Penalties Compensation And Adjudication  
(this chapter covers section 43 to section 47)
  - ▶ Chapter 10: The Cyber Appellate Tribunal  
(this chapter covers section 48 to section 64)
  - ▶ Chapter 11: Offences  
(this chapter covers section 65 to section 78)
  - ▶ Chapter 12: Intermediaries Not To Be Liable In Certain Cases  
(this chapter covers section 79)
  - ▶ Chapter 12A: Examiner Of Electronic Evidence  
(this chapter covers section 79A)
  - ▶ Chapter 13: Miscellaneous  
(this chapter covers section 80 to section 90)



# Salient Features

- ▶ The Act provided legal sanction to digital signatures
- ▶ It also gave electronic documents admissibility in court of law by amendment to Indian Evidence Act 1872.
- ▶ One of the objectives of the Act was to legalize Electronic Commerce.



- 
- 
- ▶ 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.



## Central Government to notify Examiner of Electronic Evidence(Sec. 79 A)

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence. Explanation.–For the purposes of this section, — **electronic form evidence** means any information of *probative value* that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.



- ▶ **Section 66 A ( Supreme Court struck it down in 2015)**

- ▶ Punishment for sending offensive messages through communication service, etc.

- ▶ Any person who sends, by means of a computer resource or a communication device,-

- ▶ a) any information that is grossly offensive or has menacing character; or

- ▶ b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by making use of such computer resource or a communication device,

- ▶ c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008)

- ▶ shall be punishable with imprisonment for a term which may extend to two three years and with fine.

# Penalties for various cyber crimes

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 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.	Imprisonment up to three years, or/and with fine up 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
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 fraudulently 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 publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to 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 predated 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 is 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 intermediary (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 2 years, or/and with fine up to ₹ 100,000

---

69	Failure/refusal to decrypt data	<p>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 States 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.</p>	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	<p>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.</p>	Imprisonment up to ten years, or/and with fine.
71	Misrepresentation	<p>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.</p>	Imprisonment up to 2 years, or/and with fine up to ₹100,000





# CERT-In Guidelines for Auditing and Logging

The logs collected from network devices, servers and systems need to be preserved for facilitating appropriate investigation, assist the Law Enforcement and to take appropriate legal action against the attackers.

The logs would provide vital clues about the attacks & attackers and would enhance the quality of evidence.



# Concluding Remarks

- ▶ We have covered the basics of IT Act 2000 and its amendments.
- ▶ We saw that IT Act has now become more broad based and includes latest technologies.
- ▶ IT Act not only provides a legal framework for dealing with cyber crimes but also provides for various bodies for compliance for its provisions.
- ▶ CERT-IN (Now ICERT ) works as a nodal agency for related policy.



# References

1. [https://indiacode.nic.in/bitstream/123456789/6819/1/indian\\_evidence\\_act\\_1872.pdf](https://indiacode.nic.in/bitstream/123456789/6819/1/indian_evidence_act_1872.pdf)
2. <https://www.meity.gov.in/content/information-technology-act>
3. [https://cert-in.org.in/PDF/it\\_amendment\\_act2008.pdf](https://cert-in.org.in/PDF/it_amendment_act2008.pdf)
4. <https://certin.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=CISG-2008-01>
5. Cyber Law and IT Protection, Harish Chander, Prentice Hall of India, 2012.
6. Sujata Pawar; Yogesh Kolekar , Essentials of Information Technology Law. Notion Press. pp. 296–306. ISBN 978-93-84878-57-3.
7. <https://www.itlaw.in>