IT Act 2000

The IT Act 2000 provides a legal framework for e-commerce and digital transactions in India by giving legal recognition to electronic records and digital signatures. Key aspects include criminalizing cybercrimes like hacking and identity theft, establishing a Cyber Appellate Tribunal to hear appeals, and promoting electronic governance. The act also addresses data protection and holds corporate entities accountable for data loss due to a lack of reasonable security measures.

The Information Technology Act, 2000, originally has 94 sections and 13 chapters covering various aspects of electronic governance, digital signatures, and cybercrimes. Key sections include Section 1 (commencement), Section 2 (definitions), Section 3 (authentication of electronic records), and Section 5 (legal recognition of electronic signatures) which lay the groundwork for e-transactions. Other important sections include Section 66, which deals with computer-related offenses like hacking, and Section 69, which gives the government the power to intercept information for national security.

Core provisions and features

Legal recognition of electronic records: The act grants legal validity to electronic records and contracts, making e-commerce legally enforceable.

Digital and electronic signatures: It recognizes electronic signatures as the legal equivalent of physical signatures and outlines their security.

Cybercrimes and penalties: The act criminalizes various offenses, including hacking, data theft, identity theft, and sending offensive messages, with associated penalties.

E-governance: It facilitates electronic filing of documents with government agencies and promotes digital transactions, improving efficiency and transparency.

Data protection: It addresses data privacy and makes it mandatory for companies to get consent before collecting personal data.

Liability protection: Section 79 provides a degree of protection from liability for intermediaries who follow due diligence guidelines.

Cyber Appellate Tribunal: Establishes a specialized body to hear appeals against orders passed by the Controller of Certifying Authorities.

Certifying Authorities: Defines the role and powers of the Controller of Certifying Authorities, a government body responsible for issuing and maintaining digital signature certificates.

Key sections: -

Foundational and procedural sections

- **Section 1: Short title, extent, commencement, and application.**
- **Section 2: Definitions of key terms used in the act.**
- **Section 3: Authentication of electronic records.**
- **Section 5: Legal recognition of electronic signatures.**
- **Section 10A: Validity of contracts formed through electronic means.**
- **Section 11: Attribution of electronic records.**
- **Section 13: Time and place of dispatch and receipt of electronic records.**

E-governance and administration

- **Section 6: Use of electronic records and signatures in government.**
- **Section 6A: Delivery of services by service providers.**
- **Section 17: Appointment of Controller and other officers.**
- **Section 18: Functions of the Controller.**

Cybercrime and offenses

- **Section 66: Deals with computer-related offenses, including hacking.**
- **Section 66B: Punishment for dishonestly receiving stolen computer resources.**
- **Section 66D: Punishment for cheating by personation using a computer resource.**
- **Section 66E: Punishment for violation of privacy.**
- **Section 66F: Punishment for cyber terrorism.**
- **Section 67: Punishment for publishing or transmitting obscene material in electronic form.**
- **Section 69: Power to issue directions for interception, monitoring, or decryption of information.**
- **Section 69A: Power to block public access to information.**

Other provisions

- **Section 43: Deals with unauthorized access and damage to computer systems.**
- **Section 70: Protection of protected systems, which are critical information infrastructure.**

Section 43: Covers penalties and compensation for damage to computer systems and data.

Section 66: Criminalizes the act of hacking into a computer system.

Section 66A: Punishes the sending of offensive messages via computer or other communication devices.

Section 79: Provides protection to intermediaries from liability.