# UNIT-II

**Ethics in Cyber Security & Cyber Law:** Privacy, Intellectual Property, Professional Ethics, Freedom of Speech, Fair User and Ethical Hacking, Trademarks, Internet Fraud, Electronic Evidence, Cybercrimes.

## 1 Information Technology (IT) Act, 2000

### *1.1 Introduction

The **Information Technology Act, 2000** was the first law in India to address the **legal recognition of electronic documents**, **cybercrimes**, **digital signatures**, and **e-commerce**. It was enacted on **17th October 2000** and has since been amended to keep pace with evolving technology.

### *1.2 Objectives of the IT Act

- **Legal recognition** of electronic records and digital signatures.
- Facilitate **electronic filing of documents** with Government agencies.
- Prevent and punish **cybercrime** (e.g., hacking, identity theft, cyberstalking).
- Ensure **cybersecurity** and integrity of electronic data.
- Promote **e-governance** and **online transactions**.
- Protect privacy and confidentiality of data.

### *1.3 Key Terminologies

| Term | Meaning |
|---|---|
| **Electronic Record** | Data generated, received or stored electronically. |
| **Digital Signature** | Authenticates electronic documents using asymmetric cryptography. |
| **Cybercrime** | Any unlawful act involving a computer or network. |
| **Certifying Authority** | Body authorized to issue digital certificates. |
| **Intermediary** | Includes ISPs, web-hosting providers, social media platforms, etc. |

## 1.4 Structure of the IT Act, 2000

| Chapter | Content |
|---|---|
| I | Preliminary (Definitions, Scope) |
| II | Digital Signatures and Authentication |
| III | Electronic Governance (filing, retention of e-records) |
| IV | Attribution, Acknowledgement, and Dispatch of e-Records |
| V | Secure Electronic Records & Secure Digital Signatures |
| VI | Regulation of Certifying Authorities |
| VII | Digital Signature Certificates |
| VIII | Duties of Subscribers |
| IX | Penalties and Compensation |
| X | Adjudication |
| XI | Cyber Regulations Appellate Tribunal |
| XII | Offences |
| XIII | Network Service Providers |
| XIV | Miscellaneous |

## Chapter I: Preliminary (Section 1 - 2)

### Section 1: Short Title, Extent, Commencement and Application

- **Title**: Information Technology Act, 2000
- **Applies to**: All of India and outside India (if cybercrime affects India)
- **Example**: If a hacker in the USA targets an Indian website, they can be tried under this act.

### Section 2: Definitions

- **Key Terms**: Access, Digital Signature, Computer, Cyber Cafe, Data, Information, etc.
- **Example**: "Computer Contaminant" refers to any code designed to destroy, access or modify information.

## Chapter II: Digital Signatures (Section 3 - 10A)

### Section 3: Authentication of Electronic Records

- Digital signatures ensure that the document is genuine and not altered.
- **Example**: Signing a PDF with Aadhaar e-sign.

### Section 4 - 10A:

- **Legal Recognition of Electronic Records and Signatures**
- **Use in contracts**
- **Retention of electronic records**
- **Case Law**: *State of Delhi v. Mohd. Afzal* - accepted email as valid evidence.

## Chapter III: Electronic Governance (Section 11 - 18)

### Highlights:

- Government can accept electronic records and signatures.
- **Example**: Income Tax returns filed online are legally valid.

## Chapter IV: Attribution, Acknowledgement and Dispatch of Electronic Records (Section 19 - 22)

- Defines when an electronic message is sent/received.
- **Example**: Email receipt timestamp is legally valid.

## Chapter V: Secure Electronic Records (Section 23 - 24)

- Defines secure electronic signature and record

## Chapter VI: Regulation of Certifying Authorities (Section 25 - 42)

- Controller of Certifying Authorities (CCA) governs digital signatures.
- **Sections 27-34** cover licensing, duties, and audit of certifying authorities.
- **Example**: Aadhaar Digital Signature Authority.

## Chapter VII: Digital Signature Certificates (Section 35 - 39)

- Issue, suspension, and revocation of digital signature certificates.
- **Example**: Banks revoking DSCs upon fraud.

## Chapter VIII: Duties of Subscribers (Section 40 - 42)

- Protecting private keys
- Reporting compromise

## Chapter IX: Penalties, Compensation, and Adjudication (Section 43 - 47)

Section 43: Penalty for Damage to Computer, Computer System

- Unauthorized access, downloading, virus infection: up to Rs. 1 crore compensation
- **Case**: *Avnish Bajaj v. State* (Bazee.com case)

Section 43A: Compensation for failure to protect sensitive data - Companies must secure user data

Section 45: Penalty for failure to furnish information

Section 46 - 47: Adjudication and calculating compensation

## Chapter X: Cyber Appellate Tribunal (Section 48 - 64)

- Tribunal hears appeals from adjudicating officers
- **Example**: Disputes between users and certifying authorities

## Chapter XI: Offences (Section 65 - 78)

Section 65: Tampering with computer source documents

- **Punishment:** 3 years or fine or both

Section 66: Hacking

- **Case**: *Sony India Hacking Case*
- **Punishment**: 3 years and/or Rs. 5 lakh fine

Section 66A: Sending offensive messages (struck down in 2015 by SC in *Shreya Singhal case*)

Section 66B-F: Identity theft, cyber terrorism, cheating via computer

- **Example**: Fake banking sites

Section 67: Publishing obscene material online

- **Case**: *Delhi Public School MMS scandal*

Section 70: Protected System

- Power plants, defense computers

**Section 72: Breach of confidentiality**

- **Example**: Government employee leaking Aadhaar info

### Chapter XII: Intermediaries (Section 79)

- Safe harbor for platforms like Facebook, Google if they act on illegal content reports

### Chapter XIII: Miscellaneous (Section 80 - 94)

**Section 80: Powers of police to enter and arrest**

- Without warrant in cyber crimes

**Section 81 - 94:**

- Includes protection for actions in good faith
- Power to make rules

**Example**: IT (Reasonable Security Practices) Rules, 201

## *5. Important Sections of the IT Act For Cyber Security.

| Section | Description | Example/Case |
|---|---|---|
| 43 | Damage to computer/network without permission (civil offense) | Unauthorized access in office systems. |
| 66 | Hacking (criminal offense) | Hacking email accounts. |
| 66C | Identity Theft | Stealing Aadhaar details online. |
| 66D | Cheating by impersonation using computer resources | Online fraud calls pretending to be a bank. |
| 66E | Violation of privacy (capturing photos/videos without consent) | Taking private photos through webcam hacks. |
| 67 | Publishing or transmitting obscene material | WhatsApp forwarding of adult content. |
| 69 | Government powers to intercept/decrypt information | Lawful surveillance in national interest. |
| 72 | Breach of confidentiality and privacy by service providers | ISP misusing customer data. |
| 79 | Intermediary liability | Social media platforms and responsibility for user posts. |

## *1.6 Amendments to the IT Act

**IT (Amendment) Act, 2008**

- Added new cyber offences like:
  - Cyber terrorism (Sec 66F)
  - Child pornography (Sec 67B)
  - Identity theft (Sec 66C)
  - Cyber cheating (Sec 66D)
- Introduced **data privacy safeguards**
- Strengthened **intermediary responsibilities**

## 1.7 Notable Cases

| Case | Key Point | Outcome |
|---|---|---|
| *Avnish Bajaj v. State* | Section 67 misuse (Bazee.com MMS case) | Highlighted ISP liability. |
| *Shreya Singhal v. Union of India* | Section 66A declared unconstitutional | Promoted freedom of speech. |
| *Tamil Nadu Hacking Case* | Section 66 applied on email hack | 3-year jail term given. |

## *1.8. Real-World Applications

- **E-Governance**: Income tax filing, passport applications.
- **Digital Contracts**: Legally valid with digital signatures.
- **Cybercrime Investigation**: Police use IT Act sections to file FIRs.
- **Corporate Cyber Security Policies**: Based on IT Act compliance.

## *1.9 Penalties & Punishment

| Offense | Punishment |
|---|---|
| Hacking (66) | Up to 3 years jail + fine ₹5 lakh |
| Obscenity (67) | 5 years + ₹10 lakh fine |
| Identity theft (66C) | 3 years jail + fine |
| Cyber terrorism (66F) | Life imprisonment |

Table: All 94 Sections of the Information Technology (IT) Act, 2000

| Section No. | Title/Provision | Description |
|---|---|---|
| 1 | Short title, extent, commencement and application | Defines the title of the Act, its extent, and scope of application. |
| 2 | Definitions | Provides key definitions such as access, data, computer, communication device, etc. |
| 3 | Authentication of electronic records | Legal recognition of electronic records and authentication using digital signatures. |
| 4 | Legal recognition of electronic records | Electronic records are legally valid like physical documents. |
| 5 | Legal recognition of digital signatures | Digital signatures are legally recognized if they conform to specified standards. |
| 6 | Use of electronic records and signatures in Government | Allows government to use electronic records and digital signatures. |
| 6A | Delivery of services by service provider | Electronic delivery of services is permitted by authorized service providers. |
| 7 | Retention of electronic records | Guidelines for storing electronic records for future reference. |
| 7A | Audit of documents, etc. | Allows auditing of electronic documents maintained by intermediaries. |
| 8 | Publication of rules, regulations, etc. in Electronic Gazette | Validates electronic gazettes for publishing rules and notifications. |
| 9 | Sections 6, 7 and 8 not to confer right to insist document be accepted in e-form | Does not give unconditional right to demand electronic records be accepted. |
| 10 | Power to make rules regarding digital signature | Rules for digital signature standards, processes, and usage. |
| 10A | Validity of contracts formed through electronic means | Recognizes contracts formed through electronic communication. |
| 11 | Attribution of electronic records | How electronic records are attributed to their originator. |
| 12 | Acknowledgement of receipt | Guidelines for receipt confirmation of electronic communications. |
| 13 | Time and place of dispatch and receipt of electronic record | Legal clarity on when and where electronic communication is considered sent/received. |
| 14 | Secure electronic record | Definition and criteria of a secure electronic record. |
| 15 | Secure digital signature | Standards and conditions for secure digital signatures. |
| 16 | Security procedure | Guidelines on secure procedures for electronic communications. |
| 17 | Appointment of Controller | Establishes the Controller of Certifying Authorities. |
| 18 | Functions of Controller | Defines the roles and duties of the Controller. |
| 19 | Recognition of foreign Certifying Authorities | Legal recognition of foreign digital certifying authorities. |

| | | |
|---|---|---|
| 20 | Controller to act as repository | Controller maintains a database of digital signatures and related certificates. |
| 21 | License to issue digital signature certificate | Process for granting licenses to Certifying Authorities (CAs). |
| 22 | Application for license | Procedure for applying for a license to issue digital signatures. |
| 23 | Renewal of license | Conditions for renewal of CA licenses. |
| 24 | Procedure for grant or rejection of license | Guidelines for accepting or rejecting applications for CA license. |
| 25 | Suspension of license | Allows suspension of CA license under certain conditions. |
| 26 | Notice of suspension or revocation | Requires notice to be issued if license is suspended or revoked. |
| 27 | Power to delegate | Controller may delegate certain powers to other officers. |
| 28 | Power to investigate contraventions | Authorizes investigation into non-compliance or breaches. |
| 29 | Access to computers and data | Authorizes access to computer systems for investigation. |
| 30 | Certifying Authorities to follow certain procedures | Standard procedures to be followed by CAs. |
| 31 | Certifying Authority to ensure compliance of the Act | Certifying Authorities must comply with all provisions of the IT Act. |
| 32 | Display of license | CAs must publicly display their license. |
| 33 | Surrender of license | Allows voluntary surrender of a license by a CA. |
| 34 | Disclosure | Guidelines for disclosure of information by Certifying Authorities. |
| 35 | Power of Controller to give directions | Controller can issue binding directions to CAs. |
| 36 | Appeal to Cyber Appellate Tribunal | Right to appeal decisions of the Controller. |
| 37 | Compounding of contraventions | Permits settling of offenses without litigation under certain terms. |
| 38 | Cyber Appellate Tribunal | Establishes a tribunal to hear appeals related to IT Act. |
| 39 | Qualifications for appointment as Presiding Officer | Criteria for selecting presiding officers for the tribunal. |
| 40 | Term of office | Specifies term duration for the tribunal members. |
| 41 | Salary, allowances and other terms of service | Details on remuneration of tribunal members. |
| 42 | Filling up of vacancies | Guidelines for replacing presiding officers in case of vacancy. |
| 43 | Penalty and compensation for damage to computer systems | Covers hacking, data theft, viruses, unauthorized access, etc. |
| 43A | Compensation for failure to protect data | Holds companies liable for data breach or poor data protection. |
| 44 | Penalty for failure to furnish information | Fine for failure to provide required information to authorities. |

| | | |
|---|---|---|
| 45 | Residuary penalty | Penalty for contraventions not specifically mentioned in the Act. |
| 46 | Power to adjudicate | Allows appointment of adjudicating officers to handle violations. |
| 47 | Factors to be taken into account by adjudicating officer | Guidelines for determining the quantum of penalty. |
| 48–64 | [Omitted or Repealed Sections] | These sections were repealed or merged under IT (Amendment) Act 2008. |
| 65 | Tampering with computer source documents | Criminal offense to modify or destroy computer source code. |
| 66 | Computer related offenses | Covers hacking and other cyber offenses. |
| 66A | Punishment for sending offensive messages electronically (Struck Down) | Declared unconstitutional by Supreme Court in 2015. |
| 66B | Dishonestly receiving stolen computer resource or communication device | Punishment for knowingly receiving stolen data/devices. |
| 66C | Identity theft | Punishment for using someone else’s digital identity (e.g., passwords, biometrics). |
| 66D | Cheating by personation using computer resource | Phishing, online fraud, etc. |
| 66E | Violation of privacy | Punishment for capturing or sharing private images without consent. |
| 66F | Cyber terrorism | Covers attacks intended to threaten national security or cause fear. |
| 67 | Publishing or transmitting obscene material in electronic form | Penalizes sharing pornographic content online. |
| 67A | Material containing sexually explicit act | Enhanced punishment for graphic content. |
| 67B | Child pornography | Punishment for child sexual abuse material. |
| 68 | Power of Controller to give directions | Directions to CAs for compliance. |
| 69 | Power to issue directions for interception or monitoring | Allows authorized agencies to monitor internet traffic under due process. |
| 69A | Blocking public access of any information through computer resource | Legal basis for blocking websites in India. |
| 69B | Monitoring and collection of traffic data | For cyber security incident analysis. |
| 70 | Protected system | Government declares any computer system as a protected system. |
| 70A | National Nodal Agency | Appoints an agency for cyber security coordination. |
| 70B | Indian Computer Emergency Response Team (CERT-IN) | Nodal agency for cybersecurity incidents. |
| 71 | Penalty for misrepresentation | Penalty for providing false info to obtain licenses or certificates. |
| 72 | Breach of confidentiality and privacy | Unauthorized access or disclosure of personal data. |
| 72A | Disclosure of information in breach of lawful contract | Covers data leaks by service providers. |

| | | |
|---|---|---|
| 73 | Penalty for publishing false digital signature certificate | Misuse or forgery of digital certificates. |
| 74 | Publication for fraudulent purpose | Publishing a certificate for fraud or deceit. |
| 75 | Act to apply for offense outside India | Jurisdiction extends to offenses outside India affecting Indian systems. |
| 76 | Confiscation | Confiscation of devices used in cyber offenses. |
| 77 | Compensation, penalties not to interfere with other punishment | Civil penalties do not bar criminal prosecution. |
| 77A | Compounding of offenses | Allows settlement of offenses. |
| 77B | Offenses with imprisonment less than 3 years to be bailable | Clarifies bailability of minor offenses. |
| 78 | Power to investigate offenses | Police officers not below inspector rank can investigate cybercrimes. |
| 79 | Exemption from liability of intermediary in certain cases | Safe harbor for platforms like ISPs, websites under specific conditions. |
| 80 | Power of police officer and other officers to enter, search, etc. | Grants power to enter, search, seize computer systems for investigation. |
| 81 | Act to have overriding effect | IT Act overrides other conflicting laws. |
| 82 | Controller, etc., to be public servants | Officials under the Act are considered public servants. |
| 83 | Power to give directions | Central Government can issue directions for proper implementation. |
| 84 | Protection of action taken in good faith | Protection for actions taken honestly under the Act. |
| 84A | Modes or methods for encryption | Central Government may prescribe standards for encryption. |
| 84B | Punishment for abetment of offenses | Covers aiding or assisting in cybercrimes. |
| 84C | Punishment for attempt to commit offenses | Covers attempt to commit cybercrimes. |
| 85 | Offenses by companies | Defines corporate liability for cyber offenses. |
| 86 | Removal of difficulties | Government can resolve implementation issues. |
| 87 | Power of Central Government to make rules | Central Government's rule-making power. |
| 88 | Constitution of Advisory Committee | To advise the government on cyber law matters. |
| 89 | Power of Controller to make regulations | Controller’s power to regulate Certifying Authorities. |
| 90 | Power of State Government to make rules | State rule-making power. |
| 91–94 | Miscellaneous | Includes repeal of conflicting laws and transitional provisions. |

## Punishments Under the IT Act, 2000 – Section-Wise Table (Extended)

| Sec No. | Description | Punishment |
|---|---|---|
| 43 | Penalty and compensation for damage to computer, system, etc. | Compensation to affected person, up to ₹1 crore or more as adjudicated. |
| 43A | Compensation for failure to protect data | Up to ₹5 crore or more as per sensitivity and adjudication. |
| 65 | Tampering with computer source documents | Imprisonment up to 3 years, or fine up to ₹2 lakh, or both. |
| 66 | Hacking with computer systems, data alteration | Imprisonment up to 3 years, or fine up to ₹5 lakh, or both. |
| 66A (Struck down) | Sending offensive messages electronically | **Struck down by Supreme Court in 2015.** |

**The phrase "Struck down by Supreme Court in 2015" means that:**

The Supreme Court of India declared a particular law or part of a law as unconstitutional or invalid in the year 2015 — so it no longer had legal power and could not be used anymore.

**Simple Explanation:**

- The **Supreme Court** is the highest court in India.
- It has the power to **review laws** passed by Parliament or State legislatures.
- If the Court finds that a law **violates the Constitution of India**, it can **strike it down**, meaning:
  - That law becomes **null and void** (no longer in use).
  - It cannot be applied or enforced anymore.

**Example (Real Case):**

One of the most famous examples is **Section 66A of the IT Act, 2000**.

- **Section 66A** made it a crime to post any "offensive" or "annoying" content online.
- Many people were **arrested** for Facebook posts or tweets — even if they were just jokes or personal opinions.
- This was seen as a **violation of freedom of speech** (Article 19 of the Constitution).
- So in **March 2015**, the **Supreme Court struck down Section 66A**.
  - That means the Court **removed it from the law**.
  - After 2015, **no one can be punished** under Section 66A anymore.

**Summary in One Line:**

"Struck down by Supreme Court in 2015" means the top court removed that law because it was **against the Constitution or people's rights.**

| | | |
|---|---|---|
| 66B | Receiving stolen computer resource/device | Imprisonment up to 3 years, or fine up to ₹1 lakh, or both. |
| 66C | Identity theft (using digital signature, password, etc.) | Imprisonment up to 3 years, or fine up to ₹1 lakh, or both. |

| | | |
|---|---|---|
| 66D | Cheating by impersonation via computer | Imprisonment up to 3 years, or fine up to ₹1 lakh, or both. |
| 66E | Violation of privacy | Imprisonment up to 3 years, or fine up to ₹2 lakh, or both. |
| 66F | Cyber terrorism | Imprisonment for life. |
| 67 | Publishing/transmitting obscene material | Imprisonment up to 3 years (first conviction), fine up to ₹5 lakh; higher for repeat offenders. |
| 67A | Publishing sexually explicit content | Imprisonment up to 5 years, fine up to ₹10 lakh. |
| 67B | Child pornography | Imprisonment up to 5 years, fine up to ₹10 lakh. |
| 67C | Failure to maintain records by intermediaries | Imprisonment up to 3 years, and fine. |
| 68 | Failure to comply with directions of Controller | Imprisonment up to 2 years, or fine up to ₹1 lakh, or both. |
| 69 | Interception/decryption by government | Unauthorized action punishable with imprisonment up to 7 years and fine. |
| 69A | Blocking public access to online info | Non-compliance can lead to imprisonment up to 7 years and fine. |
| 69B | Monitoring traffic data by government | Unauthorized access leads to imprisonment up to 3 years and fine. |
| 70 | Protected system access without permission | Imprisonment up to 10 years and fine. |
| 70A | National Nodal Agency failure | Penalty varies by circumstances under national security rules. |
| 70B | Indian CERT (Emergency Response Team) non-compliance | Imprisonment up to 1 year, or fine up to ₹1 lakh, or both. |
| 71 | Misrepresentation or suppression of facts | Imprisonment up to 2 years, or fine up to ₹1 lakh, or both. |
| 72 | Breach of confidentiality and privacy | Imprisonment up to 2 years, or fine up to ₹1 lakh, or both. |
| 72A | Disclosure of information in breach of lawful contract | Imprisonment up to 3 years, or fine up to ₹5 lakh, or both. |

| | | |
|---|---|---|
| 73 | Publishing false Digital Signature Certificate | Imprisonment up to 2 years, or fine up to ₹1 lakh, or both. |
| 74 | Publication for fraudulent purpose | Imprisonment up to 2 years, or fine up to ₹1 lakh, or both. |
| 75 | Act to apply for offences outside India as well | Jurisdiction extends globally for Indian systems or citizens. |
| 76 | Confiscation of computer resources | Government authorized to seize in cases of violation. |
| 77 | Compensation to be civil liability | Civil remedies in addition to criminal punishment. |
| 77A | Compounding of offences | Some offences can be settled out of court. |
| 77B | Offences with imprisonment of <3 years to be bailable | Eases the bail process for lesser cyber offences. |
| 78 | Power to investigate offences | Officer not below rank of Inspector can investigate. |
| 79 | Exemption of liability for intermediaries | Intermediaries not liable if due diligence is observed. |
| 80 | Power of police to enter, search, arrest without warrant | Can act on reasonable suspicion of offence. |
| 81 | Act to have overriding effect | Supersedes conflicting laws. |
| 82–94 | Administrative and procedural provisions | Appointment of adjudicating officers, digital evidence acceptance, rules formulation, etc. |

## *1. Privacy

Privacy in the digital era refers to the **individual's right to control their personal information**—what data is collected, how it's used, who can access it, and how it's stored or shared. With the rise of digital services, users often unknowingly share sensitive data such as:

- Name, contact details
- Location
- Financial records
- Health information
- Social interactions and habits

The **core principle** is to prevent **unauthorized access, data misuse, data leaks, or surveillance** without consent. Ensuring **digital privacy** means:

- Obtaining **informed consent** before collecting data
- Using data **only for stated purposes**
- Giving users the **right to delete, access, or correct** their information

### *1.1 Types of Privacy in Cyber Space:

| Type of Privacy | Description |
|---|---|
| Information Privacy | Protection of personal data from misuse. |
| Communication Privacy | Ensures messages, calls, and emails are private (e.g., end-to-end encryption). |
| Location Privacy | Hiding or restricting real-time location tracking by apps. |
| Internet Activity Privacy | Browsing habits and search history kept secure. |

### *1.2 Real-Time Examples:

1. **WhatsApp End-to-End Encryption**
    - Messages are encrypted so that only the sender and receiver can read them.
    - Even WhatsApp or its parent company, Meta, cannot access the message content.
2. **Google's €50 Million GDPR Fine (France – 2019)**
    - Google was penalized for **not clearly informing users** how their data would be used for ads.
    - Users weren't given clear **consent options** as required under GDPR (General Data Protection Regulation).
3. **Apple's App Tracking Transparency (iOS 14.5 onwards)**
    - Apple introduced a rule that **forces apps to ask permission** to track users across other apps or websites.
    - This gave users **greater control over privacy**, reducing hidden data tracking for ads.
4. **Facebook – Cambridge Analytica Scandal**
    - Data of **87 million users** was misused for political profiling and ads without clear consent.
    - Resulted in global backlash and investigation into Facebook's data handling practices.

### *1.3 Some Indian Laws Related to Privacy:

| Law/Act | Section | Description |
|---|---|---|
| Information Technology (IT) Act, 2000 | Section 72 | Penalizes any person who has secured access to personal information without consent and discloses it. |
| Indian Constitution | Article 21 | The Right to Privacy is recognized as part of the Right to Life and Personal Liberty (declared by the Supreme Court in Justice K.S. Puttaswamy vs Union of India, 2017). |
| IT Rules (2021) | — | Mandates platforms to provide users the option to control data, withdraw consent, and demand account deletion. |
| Digital Personal Data Protection Act (2023) | — | Introduces clear rights for data principals, obligations for data fiduciaries, and penalties for breach. (Replaces older data protection guidelines.) |

### *1.4 Punishment for Privacy Violation (India)

| Section | Punishment |
|---|---|
| Section 72 – IT Act | Imprisonment up to 2 years or fine up to ₹1 lakh, or both. |
| Section 43A – Compensation | If a company fails to protect sensitive data and causes loss, they must compensate the affected party. |
| Digital Personal Data Protection Act, 2023 | Fines up to ₹250 crores for non-compliance with privacy norms. |

### 1.4 Case Study: K.S. Puttaswamy v. Union of India (2017)

- The Supreme Court of India held that the **Right to Privacy is a fundamental right**.
- This case laid the foundation for **stronger data protection laws** in India.

## *2. Intellectual Property (IP)

Intellectual Property refers to creations of the mind such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce. In the digital world, IP includes software code, multimedia content, logos, and domain names.

Cyber laws help protect intellectual property rights (IPR) in the digital space from unauthorized use, duplication, or theft. Digital IP theft is common due to the ease of copying and sharing content online.

### *1.1 Real-Time Examples:

**Example 1:** ***Software Piracy***

- Downloading or distributing paid software like Microsoft Office or Adobe Photoshop for free without a license is software piracy.

- **Case**: Microsoft filed lawsuits globally, including in India, against businesses using unlicensed software.

**Example 2:** ***Music/Video Piracy***

- Uploading Bollywood movies to torrent websites without permission violates the Copyright Act.
- **Case**: The Indian government frequently blocks pirated movie sites under orders from the High Court.

**Example 3:** ***Plagiarism of Content or Code***

- Copying source code from GitHub without proper attribution or license.
- Students submitting copied assignments from the internet also fall under digital IP violations.

**Example 4:** ***Domain Name Disputes***

- Using a domain like "goog1e.com" to deceive users and gain traffic or profits is called cybersquatting.
- **Case**: Google won a legal case under the UDRP policy to claim such deceptive domains.

### *1.2 Key Types of Intellectual Property:

| Type | Description | Cyber Example |
|---|---|---|
| **Copyright** | Protection for original works like text, music, videos, code, etc. | Downloading cracked e-books, pirated music, or software. |
| **Trademark** | Protection for logos, names, or symbols that distinguish a brand. | Using Apple's logo for your product falsely. |
| **Patent** | Protection for inventions or new methods. | Stealing software algorithm ideas filed under patents. |
| **Trade Secrets** | Confidential business information. | Hacking into a company's system to steal marketing strategy. |

### *1.3 Key Laws Related to IP:

- **Copyright Act, 1957** – Protects digital content.
- **Trademark Act, 1999** – Protects logos, brand names.
- **Patent Act, 1970** – Protects inventions (including digital ones).
- **IT Act, 2000 – Section 65**: Tampering with computer source documents.
- **IT Act, 2000 – Section 66**: Hacking of software or theft of intellectual property.

### *1.4 Punishment (Under Indian Law):

| Section | Violation Type | Punishment |
|---|---|---|
| Section 65 | Tampering with source code or software | Imprisonment up to 3 years + fine up to ₹2 lakh |
| Section 66 | Hacking digital content | Imprisonment up to 3 years + fine up to ₹5 lakh |
| Copyright Act | Piracy or illegal copying | Up to 3 years jail + fine up to ₹2 lakh |
| Trademark Act | Misuse of brand symbols | Fine and imprisonment up to 3 years |
| Patent Act | Unauthorized use of patented tech | Legal penalties including product seizure and compensation |

➤ **Focus Points:**

- Digital content is easy to copy, so protection laws are stricter.
- Ethical use of code, images, and music is mandatory in digital projects.
- Organizations must educate employees and students on IP awareness.

➤ **Notes:**

- Always use licensed software.
- Attribute authors or creators when using their content.
- For startups and tech developers, filing for patents and trademarks ensures long-term business protection.
- Websites and apps must avoid using copyrighted logos, fonts, or names without proper license.

## *3. Professional Ethics in Cyber Security

Professional ethics refers to the set of principles and standards that guide behavior in the workplace, especially for IT and cybersecurity professionals. It ensures that individuals act responsibly, protect privacy, avoid harm, and maintain integrity when handling data and systems.

Cyber professionals often deal with sensitive information and powerful tools. Ethical conduct helps prevent misuse and builds public trust in the digital ecosystem.

### *3.1 Real-Time Examples:

**Example 1:** ***Ethical Hacking vs. Malicious Hacking***

- An **ethical hacker** tests systems to find vulnerabilities **with permission**.
- A **black-hat hacker** exploits vulnerabilities **without permission** for personal gain.
- **Case**: Infosys and TCS hire ethical hackers to test their internal systems.

**Example 2:** ***Data Privacy***

- A software developer accessing users' personal messages without authorization violates ethical norms.
- **Case**: Facebook faced criticism when its employees were found listening to user audio clips.

**Example 3:** ***Plagiarism and False Certification***

- Claiming another person's code or project as your own in job interviews or submissions is unethical.
- Faking cybersecurity certifications is a serious ethical and legal issue.

### *3.2 Key Principles of Professional Ethics:

- ✓ **Integrity** - Be honest and do what is right even when no one is watching.
- ✓ **Confidentiality** - Protect user and company data; don't disclose sensitive info.
- ✓ **Accountability** - Own your actions; report and fix your mistakes
- ✓ **Respect for Intellectual Property** - Don't use or copy others' work without permission
- ✓ **Responsible Disclosure** - If you find a system vulnerability, report it ethically
- ✓ **Avoiding Conflict of Interest** - Don't mix personal gains with professional duties

### *3.4 Applicable Laws & Codes:

- **IT Act, 2000** – Provides guidelines for ethical use of computers and data.
- **ISO/IEC 27001** – Global standard for information security practices.
- **IEEE/ACM Code of Ethics** – Widely accepted ethics codes in the IT industry.
- **CERT-IN Guidelines** – Indian cybersecurity guidelines for ethical handling of incidents.

### *3.5 Punishments for Unethical Cyber Behavior:

| Violation | Applicable Law or Act | Punishment |
|---|---|---|
| Unauthorized access to data | IT Act – Section 43 | Fine up to ₹1 crore |
| Data theft or leak | IT Act – Section 66B | Imprisonment up to 3 years + fine up to ₹5 lakh |
| Identity theft | IT Act – Section 66C | Up to 3 years + ₹1 lakh fine |
| Impersonation via email or social | IT Act – Section 66D | Up to 3 years + ₹1 lakh fine |
| Misuse of company resources | As per company policies + civil liability | Termination, legal action |

## *3.6 Do's and Don'ts for Cyber Professionals:

| Do's | Don'ts |
|---|---|
| Respect user privacy | Access or sell user data |
| Report bugs to admin | Exploit bugs for profit |
| Follow NDA agreements | Share client data |
| Use licensed software | Pirate tools or scripts |
| Uphold truth in resume | Fake certificates or skills |

## 3.6 Importance of Ethics in Cybersecurity Careers:

- Builds **trust** with clients and users.
- Ensures **legal safety** and compliance.
- Prevents **reputation damage** to individual and organization.
- Leads to better **career growth** and international opportunities.

> *Ethics is not just legal—it's moral. Always ask: **"Is this right, fair, and safe?"***

## 3.7 Real-Time Examples / Case Studies:

- **Case Study 1: Edward Snowden (USA, 2013)**: Edward Snowden, a former NSA contractor, leaked classified government surveillance documents to the media. While he claimed to expose unethical practices, the U.S. government viewed it as a serious breach of ethics and national security laws.
  **Focus:** Ethics vs. Whistleblowing vs. National Security.
- **Case Study 2: Infosys Employee Insider Trading (India, 2019)**: A few senior Infosys employees were found leaking financial earnings data to external traders for personal gain. It violated company ethics, confidentiality clauses, and SEBI regulations.

  They were suspended and prosecuted.
  **Focus:** Breach of trust and confidentiality for financial benefit.
- **Case Study 3: Facebook-Cambridge Analytica Data Scandal (2018**

  A data firm, Cambridge Analytica, misused personal data of millions of Facebook users to influence political campaigns. Facebook failed to protect users' data ethically. Both firms were fined and globally criticized.

  **Focus:** Negligent handling of user data and violation of user consent.
- **Case Study 4: Uber Data Breach Cover-Up (USA, 2016)**

  Hackers stole data of 57 million Uber users and drivers. Uber paid hackers to hide the breach and didn't inform authorities. When discovered later, Uber was fined and the Chief Security Officer was charged.

**Focus:** Unethical response to cybersecurity breach and legal non-compliance.

- **Case Study 5: Engineer Disabling Brake System in Smart Cars (Fictional Scenario for Class Use)**

  A developer working for a smart car company created a backdoor to remotely control brakes for testing but didn't document or inform management. A hacker exploited this and caused an accident.

  **Focus:** Lack of responsibility, poor documentation, and ethical lapse in critical systems.

## 3.8 Key Principles of Professional Ethics:

| Principle | Description |
|---|---|
| Integrity | Be honest and truthful in all professional actions. Avoid manipulation or concealment. |
| Confidentiality | Respect and protect confidential information of users, clients, and organizations. |
| Accountability | Take full responsibility for your actions and the outcomes of your work. |
| Respect for Law | Follow all applicable laws and regulations when working with digital systems. |
| Avoid Conflict of Interest | Don't misuse position or access for personal or external benefit. |
| Transparency | Be open about security flaws, limitations, or breaches — don't hide them. |
| Continuous Learning | Stay updated with evolving threats and tools; follow best practices in cybersecurity. |

## 3.9 Important Ethical Guidelines & Frameworks:

| Organization | Ethical Code |
|---|---|
| ACM (Association for Computing Machinery) | Code of Ethics and Professional Conduct for computer professionals. |
| IEEE Code of Ethics | Emphasizes trust, safety, honesty, and societal welfare in engineering practices. |
| CSI (Computer Society of India) | Provides guidance to IT professionals on ethical decision-making. |
| ISACA / (ISC)² | Ethical standards for cybersecurity professionals (e.g., CISM, CISSP certifications). |

## *4. Freedom of Speech & Fair Use in Cyber Space

### *4.1 Freedom of Speech:

- It is a **fundamental right** under **Article 19(1)(a)** of the Indian Constitution.
- It gives citizens the **right to express their views** freely in public, including online platforms like Facebook, Twitter, blogs, YouTube, etc.
- But this right is **not absolute** – there are **reasonable restrictions** in the interest of:
    - Public order
    - Decency and morality
    - National security
    - Defamation
    - Hate speech and communal harmony

### *4.2 Fair Use:

- Refers to using **copyrighted content** (like text, images, videos) **without permission**, but **under certain limits**, like:
    - Teaching
    - Research
    - News reporting
    - Commentary
    - Parody

### *4.3 Real-Time Examples:

| Scenario | Explanation |
|---|---|
| Tweet against govt policy | Allowed under freedom of speech if not abusive or inciting violence. |
| Sharing memes using movie scenes | Allowed under fair use for satire, but only to a limited extent. |
| YouTuber using music clips in videos | Can claim fair use, but overuse can lead to copyright strikes. |
| Writing blog posts critiquing companies | Legal under free speech if facts are true and not defamatory. |

## *4.4 Relevant Indian Laws:

| Law / Act | Purpose |
|---|---|
| **Article 19(1)(a)** of Constitution | Grants right to freedom of speech and expression |
| **IT Act, 2000** – Section 66A *(struck down)* | Previously punished "offensive" messages online |
| **IPC Section 295A** | Punishes deliberate insult to religion |
| **Copyright Act, 1957** – Section 52 | Lists conditions for **fair use** of copyrighted material |
| **Defamation Laws (IPC Section 499 & 500)** | Punish damaging someone's reputation with false statements |

## *4.5 Punishments for Misuse:

| Violation | Section | Punishment |
|---|---|---|
| Spreading hate speech online | IPC 153A / 505 | Up to 3 years + fine |
| Posting defamatory content online | IPC 499/500 | Up to 2 years + fine |
| Hurting religious sentiments | IPC 295A | Up to 3 years + fine |
| Copyright violation | Copyright Act – Section 63 | 6 months to 3 years + fine up to ₹2 lakh |
| Obscene posts on social media | IT Act Section 67 | Up to 5 years + ₹10 lakh fine (for repeated offense) |

## *4.6 Limitations of Free Speech (Reasonable Restrictions)

| Not Allowed | Example |
|---|---|
| Defamation | Publishing false news about a public figure |
| Obscenity | Posting pornographic content online |
| Hate Speech | Calling for violence against religious groups |
| Inciting Riots | Using platforms to provoke riots |
| National Security Threats | Sharing military secrets or propaganda |

## 4.7 Do's and Don'ts on Social Media:

| Do's | Don'ts |
|---|---|
| Share opinions respectfully | Troll or abuse individuals |
| Use content under fair use limits | Reupload full movies/music illegally |
| Criticize with facts and proof | Spread fake news or rumors |
| Give credits to original creators | Claim others' work as your own |

## 4.8 Case Study:

**Shreya Singhal vs. Union of India (2015)**

- Section 66A of the IT Act was struck down by the Supreme Court as **unconstitutional** because it curbed free speech arbitrarily.
- Important victory for **digital freedom of expression** in India.

• Case **Study 1: Twitter Ban in Nigeria (2021)**

After Twitter deleted a tweet by the Nigerian president for violating rules, the Nigerian government banned Twitter, citing national interest. This raised global concerns over digital freedom of speech vs. government control.

**Focus:** Government censorship vs. platform moderation.

• Case **Study 2: Munawar Faruqui (India, 2021)**

Comedian Munawar Faruqui was arrested for allegedly making remarks on religion during a live show. This incident triggered debates on artistic freedom, freedom of expression, and the legal limits of speech.

**Focus:** Cultural sensitivity vs. free expression in digital media.

• Case **Study 3: Arab Spring & Social Media (2010–2012)**

In several Middle Eastern countries, social media platforms were used by citizens to organize protests against oppressive governments. This highlighted the role of digital freedom of speech in revolution and democracy.

**Focus:** Internet as a tool for activism and political expression.

• Case **Study 4: Facebook Hate Speech Regulation in Myanmar (2018)**

Facebook was blamed for not acting early on hate speech in Myanmar, which allegedly contributed to violence against Rohingya Muslims.

**Focus:** When freedom of speech crosses into inciting violence — need for ethical content moderation.

• Case **Study 5: Student's WhatsApp Group Chat Misunderstood (Fictional Classroom Use)**

A student in college wrote strong political opinions in a private WhatsApp group. It was leaked and led to disciplinary action. Later, the court ruled it as protected speech under

Article 19(1)(a) since there was no incitement or harm.
**Focus:** Right to personal opinions vs. institutional image.

## *5. Ethical Hacking

Ethical Hacking, also known as **penetration testing** or **white-hat hacking**, is the practice of intentionally probing systems, networks, or applications for security vulnerabilities—with the **owner's permission**. The goal is to identify and fix security flaws **before** malicious hackers (black-hats) can exploit them.

Ethical hackers use the same tools and techniques as malicious hackers but **in a lawful and responsible manner**, helping organizations strengthen their cybersecurity posture.

### *5.1 Real-Time Examples:

- **Example 1: Bug Bounty Programs**
  - Companies like Google, Facebook, and Microsoft offer rewards (bug bounties) to ethical hackers who report security flaws.
  - *Case:* In 2019, a security researcher earned $75,000 for finding a serious bug in Facebook's login system.
- **Example 2: Indian Railways Hack Prevention**
  - In 2022, an Indian ethical hacker reported a vulnerability in the Indian Railways ticketing website, preventing a possible mass data breach.
- **Example 3: Tesla Model 3 Hack**
  - Ethical hackers at the Pwn2Own contest remotely hacked a Tesla Model 3’s infotainment system. Tesla thanked the team and patched the vulnerability immediately.
- **Example 4: Aadhar Data Exposure**
  - In 2018, an ethical hacker identified a flaw in an app linked to India’s Aadhaar system. UIDAI later fixed the issue based on the alert.

### *5.2 Key Points:

- ✓ **White-Hat Hacker** - Ethical hacker who follows legal boundaries
- ✓ **Black-Hat Hacker** - Malicious hacker who breaks into systems for illegal gain
- ✓ **Grey-Hat Hacker** - Hackers who may violate laws but without malicious intent
- ✓ **Bug Bounty** - Rewards for ethical hackers who report valid security vulnerabilities

## *5.3 Key Laws Related to Ethical Hacking:

| Law / Section | Description |
|---|---|
| IT Act, 2000 – Section 43 | Penalty for unauthorized access, even if intention is good (hence, consent is essential) |
| Section 66B | Punishment for dishonestly receiving stolen computer resources or communication devices |
| Section 66F | Covers cyber terrorism – ethical hackers must avoid actions misinterpreted as cyber terrorism |
| Indian Penal Code (IPC) | Unauthorized hacking may also invite charges under IPC if without permission |

## 5.4 Important Certifications for Ethical Hackers:

| Certification | Organization |
|---|---|
| CEH – Certified Ethical Hacker | EC-Council |
| OSCP – Offensive Security Certified Professional | Offensive Security |
| eJPT – Junior Penetration Tester | eLearnSecurity |

## *5.5 Use Cases:

- **Banks:** Ethical hackers are hired to test the resilience of mobile banking apps.
- **E-commerce:** Sites like Amazon hire testers to prevent credit card fraud.
- **Airports and Airlines:** Used to test Wi-Fi and data systems for vulnerabilities.
- **Government Websites:** To secure citizen data and critical infrastructure.

## 5.6 Case Study: CEH Saves Major Company

**Company:** A major U.S. health insurance company
**Problem:** Suspected vulnerability in customer portal
**Ethical Hacker's Role:**

- Discovered a SQL Injection flaw
- Demonstrated it could expose 10 million patient records
- Helped patch it within 3 days
  **Outcome:** Avoided a massive HIPAA violation and a $20M+ fine

## *6. Trademarks

A **trademark** is a symbol, word, phrase, logo, or combination that distinguishes a company's product or service from others. Trademarks help customers **identify the brand origin**, maintain **trust**, and **protect the brand's reputation**.

In the context of **cybersecurity**, trademark issues often arise when someone uses a brand's name or logo without permission—such as in **fake websites, phishing emails, counterfeit software, or domain squatting.**

### *6.1 Real-Time Examples:

- **Example 1: Amazon Phishing Scam**
  - Cybercriminals used the Amazon logo and name to send fake emails requesting users to update payment info.
  - Victims were led to a fake site designed to steal credit card data.
  - This violated **Amazon's trademark rights** and endangered customers.
- **Example 2: Apple vs. Fake App Stores**
  - Multiple fake websites and app stores appeared using Apple's logo and interface.
  - Apple filed trademark complaints and lawsuits to shut them down.
- **Example 3: Domain Squatting – Facebook.in**
  - Cybercriminals registered domains like facebook.in, mimicking the real facebook.com.
  - Facebook filed trademark cases under **cybersquatting laws** and won domain rights.

### *6.2 Key Points:

- ✓ **Trademark -** Legal protection for brand name, logo, slogan, etc.
- ✓ **Service Mark -** Same as a trademark but for services instead of goods
- ✓ **Cybersquatting -** Registering domain names similar to trademarks with intent to profit
- ✓ **Infringement -** Unauthorized use of a trademark, leading to confusion or deception

### *6.3 Trademark Laws in India (IT & IPR Intersection):

| **Section / Law** | **Description** |
|---|---|
| Trademarks Act, 1999 – Section 29 | Deals with **infringement** of registered trademarks |
| Section 107 – IT Act, 2000 | Intermediary liabilities in case of trademark-infringing content |
| Cybercrime Cells + Trademark Law | Joint action taken when infringement occurs online |

| | |
|---|---|
| IN Domain Dispute Resolution Policy (INDRP) | Handles domain name conflicts involving trademarks |

### *6.4 Punishments:

| Offense | Punishment |
|---|---|
| Using a registered trademark without permission | Up to 3 years imprisonment and/or fine up to ₹2 lakh |
| Selling goods with counterfeit marks | Up to 3 years imprisonment and fine |
| Domain name squatting (IN Registry) | Domain seized; possible civil penalties or arbitration fines |

### *6.5 Use Cases:

- **E-commerce sites:** Protecting product logos from being copied on fake websites.
- **App stores:** Removing apps that copy icons or names of real brands.
- **Social media platforms:** Monitoring and reporting fake brand pages.
- **Educational institutions:** Prevent misuse of logos on unauthorized certificate-generating websites.

### 6.6 Case Study: Nike vs. Fake Website Network

**Background:**

- Nike discovered over 200 fake websites using its name and logo.
- These sites sold counterfeit shoes and used domains like nike-deals.com and nikestore-discount.org.

**Action Taken:**

- Nike filed **trademark infringement** complaints in the U.S. and India.
- Domain registrars were ordered to suspend domains and provide owner information.

**Outcome:**

- Over 190 domains were taken down.
- Customers were notified through public advisories.
- Estimated loss prevention: Over **$5 million** in counterfeit sales.

## *7. Internet Fraud:

**Internet fraud** refers to any type of **deception** conducted online with the intention of **stealing money, data, identity, or sensitive information** from individuals or organizations. It includes a wide variety of cybercrimes committed via the internet such as phishing, identity theft, credit card fraud, auction fraud, online scams, and more.

These activities often **exploit trust, fear, or urgency** to trick people into revealing private information or making financial transactions.

### *7.1 Real-Time Examples:

- **Example 1: Phishing via Fake Bank Emails**
  - Victims receive emails pretending to be from a bank (e.g., SBI).
  - They are asked to "verify account" and enter login, ATM PIN, OTP.
  - The attacker immediately transfers money from the victim's account.
- **Example 2: OLX/Fake Buyer Fraud**
  - On OLX, a fake buyer pretends to buy a product and sends a fake UPI payment screenshot.
  - Seller shares OTP or scans a QR code and loses money.
- **Example 3: Tech Support Scam**
  - Victims receive calls or pop-ups claiming their PC is infected.
  - They are told to install remote access software (e.g., AnyDesk), allowing scammers to steal data or demand money.

### *7.2 Key Types of Internet Fraud:

- ✓ **Phishing** - Fake emails/websites to steal credentials
- ✓ **Vishing** - Voice phishing (fraudulent phone calls)
- ✓ **Smishing** - Phishing via SMS messages
- ✓ **Online Shopping Fraud -** Fake e-commerce sites or non-delivery scams
- ✓ **Lottery Scams -** “You won a prize” scams demanding processing fees
- ✓ **Romance Scams -** Fraudsters build emotional connection, then ask for money

### *7.3 Relevant Laws in India:

| Law / Section | Description |
|---|---|
| IT Act, 2000 – Section 66D | Punishes cheating by impersonation using computer resources |
| Section 420 IPC | Cheating and dishonestly inducing delivery of property |
| Section 43 of IT Act | Damage or unauthorized access to computer systems |
| RBI & Banking Guidelines | Reserve Bank circulars to protect users from UPI/banking fraud |

### *7.4 Punishments:

| Offense | Punishment |
|---|---|
| Cheating by online impersonation (Sec 66D) | Up to 3 years imprisonment + fine up to ₹1 lakh |
| Financial fraud under IPC 420 | Up to 7 years imprisonment + fine |
| Online identity theft (Section 66C) | Up to 3 years + fine up to ₹1 lakh |

### *7.5 Use Cases & Applications:

- **Banks**: Use AI-based fraud detection systems for unusual transactions.
- **E-commerce**: Block suspicious sellers, verify users via KYC.
- **Telecom**: Detect and shut down fraud call centers (vishing).
- **Awareness Campaigns**: RBI, CERT-IN, and police run awareness ads on fraud prevention.

### 7.6 Case Study: ₹76 Lakh Fraud via WhatsApp Job Offer Scam

**Background:**

- Victim received a WhatsApp message offering a "part-time remote job" for liking YouTube videos and reviewing products.
- She was added to a Telegram group and paid small tasks initially.
- Later asked to "invest" money to earn more rewards.

**Action Taken:**

- She ended up paying ₹76 lakh in multiple transfers.
- FIR filed under **Section 420 IPC** and **Section 66D IT Act**.
- The Telegram group and fake accounts were traced to foreign IPs.

**Outcome:**

- Cyber Police froze remaining scam-linked bank accounts.
- Victim recovered ₹9 lakh; investigation ongoing.

## *8. Electronic Evidence

**Electronic Evidence** refers to **any digital data** that can be used in a **court of law** to prove or disprove a fact in a case. It includes emails, chat logs, call records, mobile data, social media activity, CCTV footage, computer files, metadata, and logs from digital devices or networks.

It plays a **critical role in cybercrime investigations**, civil cases, and criminal cases by helping to establish timelines, intent, identity, and communication patterns.

## *8.1 Real-Time Examples:

- **Example 1: WhatsApp Chats in Drug Case**
  - In Bollywood drug-related investigations, **WhatsApp chats** and deleted messages were retrieved as electronic evidence.
- **Example 2: Email as Evidence in Harassment**
  - In a workplace harassment case, emails sent by the accused were presented as evidence to prove continuous mental abuse.
- **Example 3: CCTV & Mobile Location**
  - In a theft case, the accused's **location data** and **CCTV footage** were used to place him at the crime scene.

## *8.2 Types of Electronic Evidence:

- ✓ **Documentary -** Emails, Outlook messages ,PDFs, invoices, Word Files- .doc, .docx
- ✓ **Transactional Logs -** Call Detail Records (CDR), system logs, ATM Logs-Withdrawals, deposits
- ✓ **Multimedia -** Photos, audio/video files, CCTV
- ✓ **Metadata -** Timestamps, location tags
- ✓ **Cloud Evidence -** Google Drive files, Dropbox data
- ✓ **Social media -** Facebook/Instagram/Twitter messages
- ✓ **Chat History** - WhatsApp, Telegram, Messenger
- ✓ **Spreadsheets** - Excel (.xls, .xlsx) files
- ✓ **Internet History** - Google searches, visited websites
- ✓ **Database Files** - SQL or Oracle data
- ✓ **Computer Memory** - RAM or hard disk contents
- ✓ **Backup Files** - Stored copies from cloud or system
- ✓ **GPS Tracks** - Google Maps location history

## *8.3 Relevant Laws in India:

| Law / Section | Description |
|---|---|
| Section 65B of Indian Evidence Act | Describes how electronic evidence must be authenticated |
| Section 66 of IT Act | Deals with computer-related offences |
| Section 43 of IT Act | Unauthorized access or damage to data |
| Section 91 of CrPC | Used to summon documents/electronic records in court |
| Section 67C of IT Act | Mandates preservation of digital records by intermediaries |

## *8.4 Punishments for Tampering or Misuse:

| Offense | Punishment |
|---|---|
| Tampering with digital evidence | Up to 3 years imprisonment + fine (under IPC 204) |
| Unauthorized data access or alteration | Up to 3 years + fine (Section 66 IT Act) |
| Failure to preserve logs (by ISPs, etc.) | Fine + cancellation of license (Section 67C IT Act) |

## *8.5 Use Cases & Applications:

- **Courts**: Accept authenticated printouts or soft copies under Section 65B.
- **Police/Cyber Cells**: Recover deleted messages, metadata, and GPS data during investigations.
- **Corporates**: Use employee system logs in internal inquiries.
- **Forensics**: Digital forensics labs extract hidden or deleted files using forensic tools.

## 8.6 Why is it Important?

- It **proves** what happened and when.
- It can help **catch criminals**.
- It shows **communication or activity logs** (like who messaged whom and what time).

## 8.7 Case Study: Delhi Corporate Espionage Case (2015)

**Background:**

- Confidential petroleum ministry documents were being leaked to corporate firms.
- Investigation led to the arrest of energy consultants and ministry officials.

**Electronic Evidence:**

- Recovered **email exchanges**, **mobile phone call logs**, and **scanned confidential files**.
- **CCTV footage** from ministry premises confirmed unauthorized entry.

**Legal Outcome:**

- Case charged under **Section 420 IPC**, **Section 66 IT Act**, and **Official Secrets Act**.
- Electronic evidence helped track the timeline of the breach and identify culprits.

## 8.8 Real-Time Examples (Case Studies):

1. **WhatsApp Chats in Court**
   In many court cases, screenshots of WhatsApp messages have been used as proof of threats, cheating, or fraud.

2. **Delhi Court Case on Email Evidence**
   A person was caught leaking official secrets via email. The court accepted the email and IP address logs as valid proof.

3. **CCTV Used in Cyber Cafe Fraud**
   CCTV footage helped police find the criminal in a scam that happened in a cyber café.

4. **GPS Tracking in Kidnapping Case**
   Police used the location data from the suspect's phone to trace his movement and find the kidnapped victim.

## 8.9 Real-Time Examples (Case Studies):

### Case Study 1: WhatsApp Chats Used in Dowry Harassment Case

*Location:* Delhi, India

*Year:* 2020

Case Summary:

A woman filed a complaint against her husband and in-laws under the **Dowry Prohibition Act** and **Section 498A (Cruelty by Husband)**. She said her husband and his family were mentally torturing her for money and gold.

**Electronic Evidence Used:**

- WhatsApp chats where the husband demanded dowry and threatened her.
- Audio recordings of calls with abusive language.
- Screenshots and timestamps were submitted with a certificate under **Section 65B** of the **Indian Evidence Act**.

**Court Judgment:**

The court **accepted the digital chats as valid evidence**, and the husband was charged. The in-laws were warned.

### Case Study 2: Email Used to Prove Corporate Espionage

***Location:* Bangalore, India**

***Year:* 2018**

**Case Summary:**

An IT employee was found **leaking confidential source code** and customer data to a competitor. The company noticed unusual logins and file downloads.

**Electronic Evidence Used:**

- Email conversations with the rival company.

- Company server logs showing download activity.
- Deleted files recovered using forensic software.

**Court Judgment:**

Under **IT Act 2000 – Section 72 (Breach of Confidentiality)**, the employee was arrested. The court held him guilty using electronic evidence, including email headers, file logs, and metadata.

### Case Study 3: GPS Data Used in Kidnapping Case

***Location:*** **Mumbai, India**

***Year:*** **2017**

**Case Summary:**

A 9-year-old child was kidnapped from school. Police had no eyewitnesses but traced the suspect's phone.

**Electronic Evidence Used:**

- GPS data from the accused's phone.
- Location history from Google Timeline (Google Account).
- CCTV footage near the crime location.

**Court Judgment:**

GPS records showed the suspect's route matched the time and place of the kidnapping. Police used this along with CCTV to convict the kidnapper.

### Case Study 4: Digital Photo Metadata Solved a Murder Case

***Location:*** **Tamil Nadu, India**

***Year:*** **2015**

**Case Summary:**

A person was murdered, and the suspect claimed he was not at the scene. But a **selfie posted on Facebook** helped reveal the truth.

**Electronic Evidence Used:**

- A selfie taken by the suspect with a timestamp and geolocation tag.
- The photo showed he was near the victim's house at the exact time of death.
- Metadata (EXIF data) was extracted from the image.

**Court Judgment:**

The court admitted the **digital photo metadata** under **Section 65B**, and the person was convicted of murder.

### Case Study 5: Internet History Used in Cyberbullying Case

***Location:*** **Hyderabad, India**

***Year:*** **2022**

**Case Summary:**

A teenager was cyberbullied with fake profiles on Instagram. The victim's mental health suffered badly.

**Electronic Evidence Used:**

- IP address tracking with help from Instagram.
- Browser history and deleted messages recovered from suspect's laptop.
- Chat logs with abusive language.

**Court Judgment:**

The suspect was a classmate. He was caught using browser history and login data. The Juvenile Court ordered cyber counseling and social media ban.

### Case Study 6: ATM Transaction Logs in Fraud Case

***Location:*** **Pune, India**

***Year:*** **2019**

**Case Summary:**

A man complained about **Rs. 50,000 withdrawn from his account** without his knowledge. He said he never shared his PIN.

**Electronic Evidence Used:**

- ATM transaction logs.
- CCTV footage from ATM showing someone using a duplicate card.
- GPS location of victim showed he was at work at that time.

**Court Judgment:**

The court ruled in favor of the victim. The bank had to refund the amount as fraud was proven using ATM logs and location mismatch.

### Case Study 7: CCTV and Chat History in Workplace Harassment Case

***Location:*** **Gurugram, India**

***Year:*** **2021**

**Case Summary:**

An employee filed a sexual harassment complaint against her manager.

**Electronic Evidence Used:**

- Internal office CCTV recordings.
- Chat messages and emails from the manager with inappropriate content.
- Witness testimony supported the digital proof.

**Court Judgment:**

The Internal Complaints Committee and court took strict action. The manager was terminated, and the case was taken forward under **POSH Act**.

## *9 Cybercrimes

Cybercrimes are criminal activities carried out using computers, networks, or the internet. These crimes target individuals, organizations, or even governments by stealing, damaging, or disrupting digital information and systems.

Cybercrimes can be categorized into:

- **Crimes against individuals** (e.g., cyberstalking, identity theft)
- **Crimes against property** (e.g., hacking, ransomware)
- **Crimes against government/society** (e.g., cyber terrorism)

### 9.1 Real-Time Examples:

1. **Ransomware Attack:** Hackers lock hospital records and demand money to unlock them.
   - *Example:* The WannaCry ransomware attack in 2017 affected over 200,000 computers across 150 countries.
2. **Phishing Scams:** Fake emails that look real trick people into giving passwords or banking info.
   - *Example:* An email pretending to be from a bank asking you to “verify your account” is a phishing attack.

3. **Cyberbullying on Social Media:** Posting harmful or threatening messages online to harass someone.

4. **ATM Skimming:** Devices placed on ATMs steal card data when users swipe their cards.

5. **Online Job Frauds:** Fake companies ask for money or personal details in return for job offers.

## *9.2 Common Types of Cybercrimes:

| Type of Cybercrime | Description |
|---|---|
| **Phishing** | Sending fake emails to steal personal data. |
| **Hacking** | Unauthorized access to computer systems. |
| **Identity Theft** | Stealing someone's personal data and impersonating them. |
| **Cyberstalking** | Harassing or threatening someone online. |
| **Malware Attacks** | Using viruses, worms, or ransomware to harm systems. |
| **Denial of Service (DoS)** | Attacking servers to make a service unavailable. |
| **Data Breach** | Exposing sensitive or confidential data. |
| **Cyber Terrorism** | Using the internet to carry out political or ideological attacks. |

## *9.3 Key Cyber Laws in India:

| Law / Section | Description |
|---|---|
| **IT Act, 2000 - Sec 43** | Penalty for damage to computer, system or network. |
| **Sec 66** | Punishment for hacking (up to 3 years + fine up to ₹5 lakh). |
| **Sec 66C** | Punishment for identity theft (3 years + ₹1 lakh fine). |
| **Sec 66D** | Punishment for cheating by impersonation (e.g., phishing). |
| **Sec 67** | Publishing or transmitting obscene content in electronic form. |
| **IPC Sec 420** | Fraud-related cybercrimes (cheating and dishonestly inducing delivery of property). |

## 9.4 Case Study:

**Case: Pune Citibank Mphasis Call Center Fraud**

- **What Happened:** In 2005, employees at Mphasis call center in Pune used fake accounts to transfer ₹1.9 crore from Citibank customer accounts in the U.S. to India.
- **How:** They used phishing and social engineering tactics to collect customer information and gain access to the accounts.
- **Outcome:** Several employees were arrested; the case highlighted the need for stricter cybersecurity and employee background checks.
- **Impact:** This incident pushed companies to improve data access controls and implement strong audit trails.

## 9.5 Important Points to Remember:

- Cybercrimes are increasing with the rise in internet usage.
- Everyone using the internet should know basic cybersecurity hygiene (e.g., strong passwords, not clicking suspicious links).
- Government bodies like **CERT-In** (Indian Computer Emergency Response Team) help track and manage cyber threats.