SUB: Cyber Security

Unit 4 : Cybercrimes and Cyber Security: The Legal Prespectives

Prof: Morade D.S.

What is Cybercrime?

Cybercrime means **illegal activities done using computers or the internet**.
It can be divided into two main categories:

1. **Cybercrime in a restrictive sense (Computer crime):**
   - Crimes where someone attacks computer systems directly.
   - Example: Hacking into a bank's server to steal account details.
2. **Cybercrime in a general sense (Computer-related crime):**
   - Crimes where computers or networks are used as a tool to commit other crimes.
   - Example: Using a computer to spread fake news or share pirated movies.

➢ Examples of Cybercrimes:

- **Unauthorized access** → Logging into someone's email without permission.
- **Data damage** → Inserting a virus that deletes files.
- **Computer sabotage** → Shutting down a company's system to cause loss.
- **Interception of communication** → Listening to private WhatsApp or email chats.
- **Espionage** → Stealing government secrets through hacking.

➢ Computer Trespassing

- Means entering someone's computer system **without permission**.
- Example: If you hack into your college's server to check exam papers, that's computer trespassing.

Cybercrime Laws in the World

Different countries have their own **laws** to punish cybercrimes.
For example, in the **Asia-Pacific region**:

➢ Australian Cybercrime Act 2001

- Added new sections in their Criminal Code (Division 477).

Key sections:

1. **<u>This section offenses under division 477 are as bellow:</u>**

1. **Section 477.1** → Unauthorized access, modification, or impairment of a computer system.
    - Example: Hacking into a government database to steal records.
2. **Section 477.2** → Unauthorized modification of data to cause harm.
    - Example: Changing exam results in a university system.
3. **Section 477.3** → Unauthorized impairment of electronic communication.
    - Example: Blocking a hospital's online system so that emergency services can't function.

2. <u>Cybercrime Offenses under Division 478 (Australian Cybercrime Act) are bellow:</u>

1. **Section 478.1** → Unauthorized access or modification of restricted data.
    - Example: A hacker breaking into a government database and changing citizens' records.
2. **Section 478.2** → Unauthorized impairment of data in a computer disk.
    - Example: A virus that corrupts important files in a company's hard drive.
3. **Section 478.3** → Possession or control of data with intent to commit crime.
    - Example: Storing stolen credit card details on your computer to use later.
4. **Section 478.4** → Producing, supplying, or obtaining data with intent to commit crime.
    - Example: Creating fake IDs or selling hacking software online.

➢ **Powers given to law enforcement (under the Act)**

The law also gives extra powers to police and investigators, such as:

1. Taking any object/computer to another place for examination.
2. Using or operating equipment to access hidden or encrypted data.
3. Asking a person to provide any needed information.
4. Forcing a person with knowledge (like a system admin) to help unlock data.

Online Safety & Cybercrime Laws in Asia-Pacific (Section 4.2.2)

- Internet safety and laws are different across Asia-Pacific countries.
- **ICMEC (International Centre for Missing and Exploited Children)** has created a model law to protect children online, especially against pornography.
- There are regional frameworks like:
    - **APEC Privacy Framework** (Asia-Pacific)
    - **EU Data Protection Directive** (Europe)

➢ **Principles of APEC Privacy Framework (in Simple Words)**

1. **Preventing harm** → Protect people from risks like identity theft.
   Example: Stop hackers from misusing medical records.
2. **Integrity of personal information** → Keep information accurate and safe.
   Example: Correcting wrong details in a bank database.
3. **Notice** → Inform users how their data will be used.
   Example: Apps showing a privacy policy before you sign up.
4. **Security safeguards** → Protect data with security measures.
   Example: Using encryption for online payments.
5. **Collection limitations** → Collect only necessary data.
   Example: A shopping site asking for delivery address, not your religion.
6. **Access and correction** → People should see and correct their own data.
   Example: Editing your profile info in Gmail or Facebook.
7. **Uses of personal information** → Data should only be used for stated purposes.
   Example: A hospital using your phone number for medical updates, not for ads.
8. **Accountability** → Organizations must follow these rules and be responsible.
   Example: A company gets fined if it leaks customer data.
9. **Choice** → People should have options to allow or deny data use.
   Example: Choosing whether an app can access your location or not.

Computer Security Laws in Asia-Pacific

- **Countries with Strong Laws (Favorable Alignment):**
  - **Australia, New Zealand, Singapore, Taiwan, Thailand**
  - These countries have strong cyber laws covering most computer crimes.
  - *Example: In Australia, hacking, data theft, and online fraud are strictly punishable.*
- **Countries with Moderate Laws (Moderate Alignment):**
  - **China, Hong Kong, Japan, Malaysia, Philippines, South Korea, Vietnam**
  - These countries have some cybercrime laws but not as strict or complete.
  - *Example: In China and Japan, laws exist but may not cover all modern cybercrimes.*
- **Countries with Weak Laws (Weak Alignment):**
  - **India, Indonesia**
  - Laws exist, but many cybercrimes are not clearly covered.
  - *Example: India's IT Act (2000) bans hacking and online fraud but does not cover all new cybercrimes like ransomware or phishing scams fully.*

Table 4.1 (Explained in Simple Form)

Favorable Alignment (Strong laws)	Moderate Alignment (Partial laws)	Weak Alignment (Limited laws)
Australia	China	India
New Zealand	Hong Kong	Indonesia
Singapore	Japan	
Taiwan	Malaysia	
Thailand	Philippines	
	South Korea	
	Vietnam	

Why this alignment difference?

- Some countries cover all kinds of cybercrimes (like hacking, fraud, identity theft).
- Others only cover **basic crimes** (like unauthorized access).
- Example: Unauthorized access in some countries might only mean "tapping a telephone line" instead of modern hacking techniques.

Data Privacy and Data Protection

- Privacy laws are also different in Asia-Pacific.
- **Microsoft's Model Privacy Bill**: A suggested framework for countries to follow for data privacy.
- Well-developed organizations follow strict **privacy regulations** of their countries.

Fair Information Practices (FIPS)

- Before collecting personal information (like name, email, address, or financial info), companies must give a **privacy notice**.
- This ensures people know **why their data is being collected and how it will be used**.

♦ Example:
When you install WhatsApp, it shows a **privacy policy** explaining how your data (messages, phone number, contacts) will be used.

Spam Laws

- **Spam = Unsolicited Bulk E-Mail (UBE)** or **Unsolicited Commercial E-Mail (UCE)**.
  - Simply: Spam = unwanted emails, usually ads or scams, sent in bulk.
- "Unsolicited" means → the sender and receiver don't have a prior relationship.
- Example: Getting hundreds of emails about fake lottery wins or medicines.

➢ **Microsoft Checklist (Opt-Out system):**

- Certain emails like **transactional or relationship messages** (e.g., bank OTPs, order confirmations) should not be considered spam.
- Anti-spam laws also fight against:
  - **Email harvesting** (collecting email IDs without permission).
  - **Dictionary attacks** (guessing possible email IDs to send bulk spam).

Anti-Spam Efforts in Asia-Pacific

- Many Asia-Pacific countries have introduced anti-spam laws.
- Strong anti-spam legislation countries:
  Japan, Australia, China, Hong Kong, New Zealand, South Korea.
- Moderate/less strict:
  Thailand, Philippines, Vietnam, Singapore.
- Still considering laws:
  Indonesia, Taiwan.

Online Protection for Children

- **ICMEC (International Centre for Missing and Exploited Children):** Defines cybercrimes related to **child pornography**.
- Many countries created laws to protect children online.
- Example:
  - **India ITA 2008** → has rules against child pornography.
  - **Japan, Philippines, Indonesia** → working on child safety laws.
- These laws are often part of broader **cyber security acts**.

➢ Anti-Spam Laws in Canada

- **Bill C-27 (2009):** Electronic Commerce Protection Act → made to fight:
  - Spam
  - Fake websites
  - Spyware
- Canada also has **PIPED Act** (Personal Information Protection and Electronic Documents Act) → protects **online privacy**, especially in **email marketing**.

 Example:

- A company cannot randomly send promotional emails unless you **consent**.
- Employee data is also protected under privacy rules.

There are two important bills:

1. **Senate Bill S-220**
   - Focuses on **Anti-Spam** and **Phishing attacks**.
   - Example: Punishing criminals who send fake bank emails to steal login info.
2. **Parliamentary Bill C-27 (2009)**
   - Government proposal to fight spam, improve coordination between agencies, and give citizens the **right to take legal action**.
   - Example: If you get spam from a company, you can complain and take legal steps.

Cybercrime and Federal Laws in the US

- **Florida Computer Crimes Act** → unauthorized computer use = crime.
- **This act covers unauthorized use of computing facilities is a crime.**
- Offenses include:

1. **Against intellectual property** → stealing software code, designs, or movies.
   Example: Pirating Hollywood movies.
2. **Against computer equipment/supplies** → damaging hardware.
   Example: Physically destroying servers in a company.
3. **Against computer users** → identity theft, fraud.
   Example: Stealing someone's credit card details online.

The EU Legal Framework for Cybercrime

- The **European Union (EU)** is an economic and political of 27 member states.
- They follow **Data Protection Directive** → regulates how personal data is collected and used.
  Example: Companies must ask permission before using your data for ads.
- Cybercrime laws are based on the **CoE's Convention on Cybercrime (2001)**.
- All EU members must punish:
  1. **Illegal access** to computer systems. (Example: Hacking into a bank system)
  2. **Illegal interception** of data. (Example: Wiretapping internet traffic without permission)
  3. **Interference with computer systems**. (Example: Spreading ransomware to lock files)

Cybercrime Legislation in Africa

- Africa is **still developing** proper cybercrime laws.
- ICT (Information and Communication Technology) is growing fast → cybercrime is also rising.
- Example: **Nigerian scams** → Fake emails promising lottery winnings or inheritance money to trick victims.

4.3 Why Do We Need Cyberlaws: The Indian Context

- Cyberlaw = laws to handle crimes and risks related to **computers and the internet**.
- Covers:
  - **Intellectual property** (copyright, software piracy)
  - **Data protection & privacy**
  - **Freedom of expression**
  - **Crimes using computers**

 The first Indian cyberlaw = **Information Technology Act, 2000 (ITA 2000)**.

- Purpose → to give legal recognition for **E-commerce** in India.
- Passed by Parliament on **17 May 2000**.

Reasons for Cyberlaws in India:

1. India had no proper laws for **internet-related crimes**.
2. Needed to support **online business and E-commerce**.
3. New threats like **cyberterrorism** emerged.
    - Example: Hacking government or banking sites to spread panic or steal money.
4. To regulate **social, political, and economic misuse of the internet**.

4.4 The Indian IT Act

- Published in **2000**.
- Purpose:
    - Legal recognition of **electronic communication** (emails, e-signatures).
    - Facilitate **E-filing** of government documents.
    - Amendments to old laws like:
        - Indian Penal Code (IPC)
        - Indian Evidence Act (1872)
        - Bankers' Books Evidence Act (1891)
        - RBI Act (1934)

Cybercrimes Punishable under Indian Laws

1. **Violation of Copyright (Section 65, Copyright Act):**
    - If someone violates copyright (e.g., pirating software, movies), punishment = **up to 2 years in jail + fine**.
2. **Sending Pornographic or Obscene Emails/Data (Section 67, IT Act):**
    - First offense → **5 years jail + ₹1 lakh fine**.
    - Repeat offense → **10 years jail + ₹2 lakh fine**.
    - Example: Sending obscene WhatsApp messages or running pornographic websites.

Cybercrimes under IT Act 2000 (Important Sections)

Section 65 – Tampering with computer source documents

- If someone **intentionally alters or destroys computer source code** (program, system files, etc.).
- **Punishment:** Up to **3 years jail** or **fine up to ₹2 lakh**, or both.
- **Example:** A software engineer deletes/modifies source code files of a company to cause damage.

Section 66 – Computer-related offences

- Covers wrongful loss/damage, deletion/alteration of data, hacking, etc.
- **Punishment:** Imprisonment up to **3 years**.
- **Example:** Hacking a bank's database and altering customer account balances.

Section 67 – Publishing/transmitting obscene material in electronic form

- If anyone **publishes or sends obscene, pornographic, or sexually explicit content** online.
- **First offence:** Up to **5 years jail + fine up to ₹1 lakh**.
- **Subsequent offence:** Up to **10 years jail + fine up to ₹2 lakh**.
- **Example:** Running a pornographic website, sharing obscene videos on WhatsApp.

Section 71 – Penalty for misrepresentation

- Giving **false information** to obtain a Digital Signature Certificate or license.
- **Punishment:** Up to **2 years jail** or **fine up to ₹1 lakh**, or both.
- **Example:** Using a fake identity to get a digital certificate for online fraud.

Section 72 – Breach of confidentiality and privacy

- If someone discloses **private electronic records, correspondence, or information** without consent.
- **Punishment:** Up to **2 years jail** or **fine up to ₹1 lakh**, or both.
- **Example:** An employee leaks company confidential emails or customer data to competitors.

Section 73 – Publishing false Digital Signature Certificate

- Publishing a **fake or unauthorized Digital Signature Certificate**.
- **Punishment:** Same as above (up to **2 years jail** or **fine up to ₹1 lakh**, or both).
- **Example:** A person issues a forged e-signature certificate to cheat others in online transactions.

Section 74 – Publication for Fraudulent Purposes

- If any person **knowingly publishes** a Digital Signature Certificate (DSC) for **fraudulent or unlawful purposes**:
  - **Punishment:**
    - Imprisonment up to **2 years**, or
    - Fine, or
    - Both

Cybercrimes under IT Act 2000 (Amendment 2008)

Section 66A – Sending offensive messages

- Covers sending offensive, false, or threatening messages via email, SMS, social media.
- **Punishment:** Up to **3 years imprisonment + fine**.
- **Example:** Sending abusive or threatening messages on WhatsApp or email.

Section 66B – Receiving stolen computer resource

- If someone **knowingly receives or uses a stolen computer/laptop/pen drive/data**.
- **Punishment:** Up to **3 years jail** or **₹1 lakh fine**, or both.
- **Example:** Buying a stolen laptop knowingly.

Section 66C – Identity theft

- Using **another person's password, digital signature, or online identity**.
- **Punishment:** Up to **3 years jail** or **₹1 lakh fine**, or both.
- **Example:** Logging into someone's Facebook using their stolen password.

Section 66D – Cheating by personation

- Pretending to be someone else online for fraud.
- **Punishment:** Up to **3 years jail** or **₹1 lakh fine**, or both.
- **Example:** A scammer creates a fake bank website to trick users.

Section 66E – Violation of privacy

- Capturing, publishing, or transmitting private images of a person without consent.
- **Punishment:** Up to **3 years jail** or **₹2 lakh fine**, or both.
- **Example:** Uploading someone's private photos without permission.

Section 66F – Cyber terrorism

- Using computers/internet to threaten sovereignty, unity, integrity, or security of India.
- **Punishment: Imprisonment for life** or **₹5 lakh fine**.
- **Example:** Hacking government/military sites to spread terror.

Section 67A – Publishing sexually explicit material

- Deals with material containing sexually explicit acts.
- **First offence:** Up to **5 years jail + ₹10 lakh fine**.
- **Second offence:** Up to **7 years jail**.
- **Example:** Uploading pornographic videos online.

Section 67B – Child pornography

- Covers publishing/transmitting material showing **child sexual acts/conduct**.
- **First offence:** Up to **5 years jail + ₹10 lakh fine**.
- **Second offence:** Up to **7 years jail**.
- **Example:** Sharing or running websites with child pornography.

Section 67C – Preservation of Records by Intermediaries

- **Meaning:** Websites, ISPs, social media platforms, etc. must **store and retain records** (logs, data, messages) for a certain time when required by law.

- **Example:** If police are investigating a cyber fraud case, WhatsApp may be asked to keep chat records for 6 months. If WhatsApp deletes them, it violates Section 67C.

Section 69A – Blocking of Websites

- **Meaning:** Government can **block access to certain websites** that may threaten national security, public order, or spread illegal content.
- **Punishment:** If anyone refuses to follow, up to **7 years imprisonment + fine**.
- **Example:** During riots, the government may block websites or social media pages spreading **fake news or hate speech**.

Section 69B – Monitoring & Collecting Traffic Data

- **Meaning:** Authorities have the power to **monitor internet traffic and data** for cyber security. If intermediaries (like Jio, Airtel, Google) do not cooperate, they can be punished.
- **Example:** To prevent a cyber-attack, CERT-In may order Airtel to share suspicious traffic logs. If Airtel refuses, it violates Section 69B.

Section 70A – National Nodal Agency (CERT-In)

- **Meaning:** The **Indian Computer Emergency Response Team (CERT-In)** is officially declared the **national agency** for protecting **Critical Information Infrastructure** (like banking, defense, power grids, telecom).
- **Example:** If there is a cyber-attack on the **Indian power grid**, CERT-In will coordinate response, issue alerts, and guide recovery measures.

Positive Aspects of the ITA 2000

1. Recognition of Electronic Records

Before ITA 2000, emails or digital documents were not accepted in courts as legal proof.
ITA 2000 made electronic records legally valid.

Example:
Earlier, if you signed a contract by email, it was not accepted in court. After ITA 2000, that email or e-document is legally valid proof.

2. Growth of E-Commerce

Earlier, there was no legal system for online transactions, so e-commerce was very slow.
ITA 2000 created a legal framework, allowing businesses to confidently do online trade.

Example:
Before 2000, Indian companies were afraid to sell online as there was no law to support it. After ITA 2000, sites like Flipkart, Amazon, and online banking became possible legally.

---

3. Use of Digital Signatures

Organizations can now use digital signatures for secure online transactions.
This ensures authenticity and security.

Example:
A company can digitally sign contracts or invoices online without needing to meet physically.

---

4. Protection Against Hacking & Data Theft

If someone breaks into a computer system and causes damage or steals data, there is now a legal remedy.
The law provides monetary compensation up to ₹1 crore (10,000,000).

Example:
If a hacker damages a company's database, the company can sue and claim financial compensation under ITA 2000.

---

5. Definition of Cybercrimes

Before ITA 2000, there was no proper law for cybercrimes.
ITA 2000 defined crimes like hacking, data theft, spreading viruses, etc., and gave legal remedies.

Example:
If someone spreads a computer virus that damages files, earlier no law covered it. After ITA 2000, it is a punishable cybercrime.

Weak Areas of the ITA 2000

1. Conflict of Jurisdiction

Cybercrimes happen across countries, but ITA 2000 applies only in India. It becomes confusing which country's law should apply.
Example: If a hacker sitting in the USA attacks an Indian bank website, Indian law alone cannot easily punish him.

---

2. Domain Name Disputes

ITA 2000 does not cover problems related to domain names (website addresses).
Example: Someone registers **www.tataelectronics.com** without being Tata company. The law does not clearly solve such disputes.

---

3. Intellectual Property Rights (IPR)

ITA 2000 does not deal much with online copyright, patents, or trademarks.
Example: If someone copies a software program or uploads pirated movies online, ITA 2000 does not give strong protection.

---

4. Limited Cybercrimes Covered

ITA 2000 does not cover all types of cybercrimes.
Example: Cyber fraud, credit card theft, identity theft, and cyberstalking are not fully covered under ITA 2000.

---

5. Privacy & Content Regulation

ITA 2000 does not properly protect user privacy or regulate harmful content.
Example: If someone leaks your personal photos or misuses your private data, ITA 2000 has weak remedies.

---

6. No Anti-Trust Provisions

ITA 2000 does not prevent monopoly or unfair competition in cyberspace.
Example: If one big company controls all online payments and blocks competitors, ITA 2000 has no strong rule to stop them.

---

7. Negotiable Instruments Not Included

ITA 2000 avoids rules related to electronic cheques or promissory notes.
Example: If you sign an e-cheque online, ITA 2000 does not clearly recognize it as valid.

Challenges to Indian Law and Cybercrime Scenario in India

The ITA 2000 made cybercrimes punishable, but there are still many **challenges**. Some crimes covered under ITA 2000 include:

---

1. Tampering with Computer Source Code

Changing or modifying the source code without permission.
Example: A hacker modifies a bank's software code to steal money.

---

2. Publishing Obscene Information Online

Uploading or sharing sexual, vulgar, or obscene content in electronic form.
Example: Sharing pornographic videos or offensive material online.

---

3. Failure to Decrypt Information when Required

If decryption is necessary for **national security, public order, or foreign relations**, and a person fails to provide it, it becomes an offense.
Example: A company refuses to give authorities access to encrypted messages that may contain terrorist plans.

---

4. Unauthorized Access to Protected Systems

Trying to enter secure systems without permission.
Example: An outsider attempting to hack into the Indian Defense Ministry's server.

---

5. Fake Digital Signature Certificates

Creating false digital signature certificates or faking authorization.
Example: A fraudster makes a fake digital certificate to look like a genuine bank website.

---

6. Violation of Privacy & Confidentiality

Using or disclosing someone's private information without consent.
Example: A hacker steals and leaks personal emails or health records.

---

7. Publication of False Digital Signature Certificates

Issuing or publishing fake digital signatures.
Example: Pretending to be a government agency by using a fake signature certificate.

---

8. Using Digital Signatures for Fraudulent Purposes

Misusing digital signatures to cheat people.
Example: Signing a fake online contract using someone else's digital signature.

Legal Drawbacks of Cybercrime in India

1. **Fear of Harassment**
   Many people don't report cybercrimes because they fear being harassed by law enforcement agencies.
   Example: A girl facing online stalking may avoid reporting it, fearing police questioning and social pressure.

---

2. **Low Awareness**
   Most people in India are not fully aware of cybercrime or how to deal with it.
   Example: Someone receiving a phishing email may not know it's a crime and just ignore it.

3. **Lack of Training in Law Agencies**
   Police and enforcement agencies are not fully trained to handle cybercrime cases.
   Example: A local police station may not know how to investigate online banking frauds.

---

4. **Cybercrime Cells Not in Every City**
   Specialized cybercrime investigation units are missing in many places.
   Example: A victim in a small town may have to travel to a metro city to file a cybercrime complaint.

---

5. **No Dedicated Cybercrime Courts**
   There are no special courts to quickly handle cybercrime cases.
   Example: A fraud case involving stolen ATM details may take years to settle in regular courts.

Ways to Overcome These Challenges

1. **Training Law Enforcement**
   Regular and updated training should be given to police and agencies.
2. **More Cyber-Savvy Judges**
   Increase the number of judges who understand cyber laws.
3. **Train Lawyers and Judges**
   Conduct cyber law workshops for the judiciary and legal professionals.
4. **Update Laws**
   Cyber laws should be revised regularly to match new crimes and technologies.
5. **Encourage Reporting**
   Victims must feel safe and confident to report without fear.

Consequences of Not Addressing These Weaknesses

- Cyber laws remain weak → E-commerce in India may not grow properly.
- India may **fall behind globally** in IT and outsourcing.
- Overseas customers may **lose trust** if data breaches keep happening.
- India may **lose its leading position** in the outsourcing market.

Example: If a U.S. company outsourcing to India faces repeated data leaks, they may shift their projects to another country like the Philippines.

Digital Signatures and the Indian IT Act (2000)

1. **What is a Digital Signature?**
    - A **digital signature** is like an **electronic fingerprint**.
    - It uses **mathematics and cryptography** to prove that a message, file, or document is genuine and has not been changed.
    - Example: When you send an email with a digital signature, the receiver can be sure it is really from you and not altered.

---

2. **Digital Signature Certificates (DSC)**
    - Just like you have an ID card in real life, in the digital world, you have a **Digital Signature Certificate (DSC)**.
    - It is issued by a trusted authority and proves your identity online.
    - Government agencies in India require DSCs for many online services (e.g., filing income tax, company registration).

---

3. **Certifying Authorities (CA)**
    - These are trusted organizations approved by the government.
    - They issue **different classes of DSCs** depending on the use:
        - For personal use (like signing documents).
        - For businesses (like company registrations).
        - For secure online transactions.

---

4. **Legal Validity in India**
    - According to the **Indian IT Act, 2000**, digital signatures have the same legal value as handwritten signatures.
    - This means a contract signed digitally is **legally valid**.

---

5. **Penalty under IT Act**
    - If someone creates or publishes a **fake digital signature certificate**, they can be punished.
    - The law ensures digital trust and prevents fraud.

Public-Key Certificate (PKC)

In cryptography, a **public-key certificate** (also called a **digital certificate**) is an **electronic document** used to prove who owns a public key.

It is basically like an **online ID card** that proves the identity of a website, company, or person in the digital world.

Main Uses

1. To prove that a public key belongs to a specific person/organization.
2. To validate the **sender's identity**.
3. To enable secure **online communication**.

Issued By

Certificates are issued by a trusted organization called a **Certificate Authority (CA)**.
Example: DigiCert, VeriSign, NIC (India)

Example in Real Life

- When you visit a secure website (**https://www.amazon.in**), your browser checks its **digital certificate**.
- This ensures you are actually connected to Amazon, not a fake site.
- Without this, hackers could create fake websites that look the same.

Important Features of a Public-Key Certificate

A certificate usually includes:

1. **X.509 version information** – defines the format of the certificate.
2. **Serial number** – unique number that identifies the certificate.
3. **Common name** – the name of the certificate holder (like a domain name or person).
4. **Public key** – the key associated with the certificate holder.
5. **Subject name** – the person/organization the certificate was issued to.
6. **Issuer information** – details of the CA who issued the certificate.
7. **Signature of issuer** – digital signature of the CA.

8. **Algorithm info** – the algorithm used for signing (like SHA-256, RSA).
9. **Extensions** – optional extra details (e.g., whether it's a CA certificate or end-user certificate).

Got it Let me explain this whole section step by step in **easy and simple language with examples**.

♦ Use of X.509 Certificates

- X.509 certificates are widely used in web browsers like **Chrome, Netscape Navigator, Internet Explorer**.
- They work with **SSL (Secure Socket Layer)** to keep online communication safe and private.

Examples of use:

1. **SSL in Browsers** → When you see **https://** in a website, it means SSL + certificate are protecting your data.
2. **Code-Signing** → When you download software, e.g., Microsoft or Java updates, a digital certificate ensures it is not tampered with.
3. **Secure E-Mail** → Standards like **S/MIME, PEM** use certificates to ensure emails are encrypted and authentic.
4. **E-Commerce** → Protocols like **SET (Secure Electronic Transaction)** use certificates to protect online shopping payments.

Representation of Digital Signatures in ITA 2000

- ITA 2000 said **digital signatures are legally valid**.
- It used **Asymmetric Cryptosystem + Hash System** for authentication.

This means:

- You use **two keys**:
  - **Private Key** → used for signing (like your secret stamp).
  - **Public Key** → used for verification (others check your signature).
- A **hash function** ensures the document has not been altered.

Example:
When you digitally sign an online agreement, your private key signs it. Anyone can check its authenticity using your public key.

♦ Drafting Mistake in ITA 2000 (Section 35(3))

- The law mistakenly required that an applicant for a **Digital Signature Certificate** must also submit a **Certification Practice Statement (CPS)**.
- This was unnecessary and complicated → it made getting certificates harder.

Example:
If you applied for a digital signature to file income tax online, you also had to submit a big technical document (CPS) which normal users couldn't prepare.

Problems with ITA 2000 (about Certifying Authorities)

- The law was **unclear** about the role and duties of **Certifying Authorities (CAs)**, who issue digital certificates.
- This confusion slowed down smooth implementation.

Impact of Oversights

- Because of drafting mistakes, there was a fear of misuse and confusion.
- To fix this, the **Ministry of IT** set up a **task force of cyber and law experts**.
- Later, the **IT Amendment Bill, 2006** was introduced based on expert recommendations.

Expert Committee Recommendations

(a) The law depended too much on **PKI (Public Key Infrastructure)**.
Problem: It allowed only one method of authentication (digital signatures).

Example: If in the future new secure methods (like biometrics or OTP-based e-signatures) come up, the old law would not allow them.

(b) The law needed to be **technology neutral**.
Meaning: It should accept any secure authentication technology, not just digital signatures.

Example: Today we use **Aadhaar e-Sign, OTPs, biometric authentication** for online verification, not only digital signatures. This is possible because later amendments made the law more flexible.

➢ PKI – Basic Components (Public Key Infrastructure)

PKI is like a **security system** that helps people and organizations use **digital signatures** and **certificates** safely.

1. **Public Key Certificate**
   - It is like an **ID card** in digital form.
   - It proves that a person owns a certain **public key**.
   - Example: Just like your Aadhaar card proves your identity in real life, a digital certificate proves your identity online.
2. **Certification Revocation List (CRL)**
   - A list of certificates that are **cancelled** and cannot be trusted anymore.
   - Example: If your driving license is lost or misused, the RTO cancels it. Similarly, if someone's private key is stolen, their certificate is revoked and added to CRL.
3. **Certification Authority (CA)**
   - A trusted body that **issues certificates** and also cancels them if needed.
   - Example: Just like the Passport Office issues passports, CA issues digital certificates.
4. **Registration Authority (RA)**
   - Works as a **middleman** between the user and the CA.
   - It checks your details before CA issues your certificate.
   - Example: Like an Aadhaar enrolment center that verifies your documents before Aadhaar is given.
5. **Certificate Repository**
   - A **secure online storage** where all valid and revoked certificates are kept.
   - Example: Like a government website where you can check if a driving license is valid or cancelled.
6. **Certain Users**
   - These are the people or systems who **use certificates** to confirm the identity of others.
   - Example: When you do online banking, the bank checks your digital certificate to ensure it's really you.

Implications for Certifying Authorities (Under IT Amendment Act, 2008)

- A **new Section 3A** was added to define **electronic signatures**.
- Now India has **two types of signatures**:
  1. **Digital Signature** (older system)
  2. **Electronic Signature** (new system)

➡Both can be used to prove your identity online.

- People may need to **get two different certificates**:
  - One for **digital signature**

    - One for **electronic signature**
    - And possibly from different CAs.
- Problem: The law was **not written clearly**, so in some places "digital signature" and "electronic signature" are written differently, creating **confusion**.

Current Scenario of Digital Signatures (Under IT Act, India)

- Because of this **confusion**, right now only **digital signatures** are being used in India.
- Electronic signatures are not fully implemented yet.

1. **Government Rules for New Systems**
    - If the government wants to start a **new authentication system**, it must publish the rules in the **Official Gazette** and present them before **Parliament**.
    - Example: If tomorrow the government introduces "Face ID authentication" for legal documents, they must officially notify it.
2. **Testing New PKI Systems**
    - Any new **PKI (Public Key Infrastructure) system** must be tested in **India** and also compared with **global standards** before it is approved.
3. **Licensing of New Systems**
    - Just like **CAs (Certifying Authorities)** are licensed now, any new system must also go through **licensing and approval**.
4. **Current Legal Position**
    - For now, **Digital Signatures** continue to be the **main legal method** of authentication in India.
    - Electronic signatures are still not fully active because the law has **gaps (lacunae)** and confusion.
5. **Definition in Law**
    - Section 2(d) says: "Affixing an electronic signature" means using **any method** to prove your identity on an electronic document.

Cryptographic Perspective on the IT Act

Here the focus is on **Non-Repudiation**.

What is Non-Repudiation?

- **Simple meaning:** You **cannot deny** what you did.
- In digital world: If you send a signed document or message, later you **cannot deny** that you sent it.

Why it is Important?

- Protects the **receiver** → The sender cannot deny sending the message.
- Protects the **sender** → The receiver cannot say, "I never got the message."

 Example:
Imagine you email a contract with your **digital signature**.

- Later, you can't say, "I never sent it."
- The other person can't say, "I never got it."

This is because the **digital signature** ensures **non-repudiation**.

Cryptographic Definitions of Non-Repudiation

1. **General Definition (Contract sense):**
    - You accept your obligation under a contract and agree to follow it.
    - Example: Signing a rent agreement digitally → you must pay the rent.
2. **E-Commerce Definition:**
    - You accept responsibility for **sending or receiving an electronic message** and you're bound by what it says.
    - Example: Ordering something online with a digital signature → you can't deny the order later.

When Can a Signature Be Denied (Repudiation Cases)?

Sometimes, even a traditional (paper) signature can be **challenged** if:

1. **Forgery** → Someone copied or faked your signature.
2. **Unfair Means** → The signature was taken under pressure, fraud, or cheating.

Example: If someone forces you to sign a blank cheque, you can deny that signature in court.

3. **Fraud by third party** – If someone cheats or manipulates the system.
4. **Undue influence by third party** – If someone forces or pressures a person into signing or sending something.

To solve such problems, **trust mechanisms** (legal + technical) are used.

Crypto-Technical Meaning of Non-Repudiation:

1. **Proof of data integrity & originality** → It proves the data hasn't been changed and it really came from the sender. Any third party can verify it.

    - Example: If you send a contract digitally signed, it proves it hasn't been tampered with.
2. **Authentication with high assurance** → Once signed, it is genuine and cannot be denied later.
    - Example: If you digitally sign an online loan agreement, you can't later say "I didn't do it."

 Indian IT Act, 2000 puts responsibility on the **person who accepts the digital signature**.

- Example: If a company accepts your digital signature on a contract, they trust it as genuine and you are bound by it.

4.8 AMENDMENTS TO THE INDIAN IT ACT

1. **Global Business Confidence**
    - India updated its IT law (IT Act 2008) so that it matches **international standards** like those in the **European Union (EU)**.
    - Reason: To assure foreign companies that their data is safe if sent to India (for outsourcing, BPO, etc.).
    - Example: A US company outsourcing customer service to India wants legal assurance that customer data won't be misused.
2. **New Offenses in ITA 2008**
    - Many new cybercrimes were added because of today's **digital economy** (online banking, e-commerce, cloud data, etc.).
3. **New Legal Definition of Cybersecurity** (Section 2(nb), ITA 2008):
    - Cybersecurity = Protecting **computers, devices, data, and networks** from:
        - Unauthorized access
        - Misuse
        - Disclosure (leak)
        - Disruption (attack)
        - Modification (tampering)
        - Destruction (deletion or corruption)
    - Example: If a hacker steals data from a company's server, it's a breach of cybersecurity.

4.8.1 Overview of Changes Made to the IT Act

1. **Section 43(j)** – Compensation for **tampering with source code**
    - If someone, without permission, **destroys, hides, steals, or alters computer source code**, they are liable.
    - Example: An employee secretly deletes or changes a company's software code to harm the company → the company can claim compensation.

2. **Section 43A** – Liability of companies for **data protection**
    - If a company (body corporate) handles sensitive personal data but fails to keep it secure → and because of this, someone suffers a loss → the company must pay damages (compensation).
    - No upper limit to liability (can be very high).
    - Example: If a bank's weak security causes customer credit card details to be leaked, the bank must compensate all affected customers.

Key Amendments in the Indian IT Act (ITA 2008)

1. Section 72A – Breach of Information Security

- If someone misuses your private information or leaks it → it is now a **criminal offense**.
- Offense is **cognizable** → police can register a case and investigate without prior permission.
- **Example:** If a telecom company employee leaks your call records to someone, he can be criminally prosecuted under Section 72A.

---

2. Sections 78 & 80 – Investigation Authority

- Earlier, only **DSPs (Deputy Superintendent of Police)** or higher could investigate IT Act cases.
- After amendment → even **Inspectors** can investigate.
- **Meaning:** Easier and quicker investigations.

---

3. Section 85 – Vicarious Liability on Companies

- If a company fails to protect data → not only the company, but also its **directors/managers** will be held guilty.
- **Example:** If a bank's server leaks customer passwords due to poor security, the **bank + top officers** can both be punished.

---

4. Section 69B – Cybersecurity Monitoring

- The government can monitor cybersecurity activities.
- If any intermediary (like internet providers, companies, etc.) **breaks these rules intentionally**, they can be jailed up to **3 years** + fined.
- **Example:** If an Internet Service Provider ignores government orders to monitor a cyberattack, they can be punished.

5. Section 70B – CERT-In (Computer Emergency Response Team – India)

- **70B(4):** CERT-In is declared the **national agency** for:
  - Analyzing cyber incidents
  - Giving alerts & warnings
  - Responding to cyberattacks
- **70B(6):** CERT-In can demand information from:
  - Service providers
  - Data centers
  - Companies, etc.
- **70B(7):** If someone refuses to provide information → punishment is:
  - Jail up to **1 year**
  - Or fine up to **₹1 lakh**
  - Or both
- **Example:** If a data center hides details about a hacking attack, it can be fined or its officers jailed.

4.8.2 Cybercafe-Related Amendments

- **Case Background (2001):**
  Two citizens wrote to the Bombay High Court complaining about **pornographic websites** being accessed freely in **cybercafes**.
- **Problem in ITA 2000:**
  - The Act did not **define cybercafe**.
  - So, cybercafes were treated only as **network service providers** under Section 79.
- **Solution in ITA 2008:**
  - Added a **clear definition of cybercafe**.
  - Cybercafes are now included under the term **intermediaries**.
  - Meaning → all **cyberlaw compliance rules** (like record-keeping, user logs, etc.) also apply to cybercafes.
- **Example:** Now a cybercafe must maintain **user identity logs** (ID proof, browsing history records) to prevent misuse for cybercrimes.

4.8.3 State Government Powers (Amendments in ITA 2008)

Earlier, under **Section 90 (ITA 2000)**, state governments could make **rules** to implement the IT Act.
After ITA 2008, these powers became **broader and stronger**.

Key Powers:

1. **Sections 69, 69A, 69B – Surveillance & Monitoring**
    - Both **Central** and **State Governments** can:
        - Appoint officers/agencies to **intercept, monitor, decrypt, or block online content**.
        - Collect **traffic data** (info about data flow, sender/receiver, etc.).
        - Define what counts as "traffic data."
    - **Example:** If a terrorist uses email/social media for planning, the government can order interception or blocking of that communication.
2. **Modified Section 70 – Protected Systems**
    - Government can declare certain **critical information infrastructures** as **"protected systems"**.
    - Only authorized persons (in writing) can access them.
    - **Example:**
        - Power grid control systems
        - Banking servers
        - Defense networks

          These can be declared as **protected systems**.
3. **Cyber Law Advisory Group**
    - State governments are encouraged to form a **group of cyber experts** to:
        - Frame detailed rules
        - Investigate cybercrimes systematically
    - **Example:** A Cyber Law Advisory Group in Maharashtra could advise police and govt. on handling cyber fraud, hacking, etc.

 Conclusion: ITA 2008 gave **more power to State Governments** for **cybersecurity implementation and crime investigation**.

4.8.4 Impact on IT Organizations

1. **Industry Response**
    - Many **IT & ITES (BPO, outsourcing)** companies were satisfied with the changes.
2. **Why?**
    - The Act now **recognizes new technologies**.
    - It addresses **increasing cybercrimes**.
    - It responds to **global concerns on data privacy/security**.
    - It gives **assurance to foreign clients** outsourcing work to India that data will be protected.
3. **Data Protection Framework**
    - ITA 2008 laid the foundation for **data protection laws** in India.
    - But → many details were left for **rule-making later** (so not everything was clear immediately).
4. **Beyond Data Protection**

- Businesses also paid attention to **other provisions** (like company liability, cybersecurity compliance, CERT-In, etc.).

 Example:

- A US bank outsourcing back-office work to an Indian BPO can now feel safer because ITA 2008 ensures:
  - Stronger data protection rules
  - Liability on companies if data leaks happen
  - Government monitoring of cybersecurity

Great Let's go step by step and explain this **in simple words with examples**.

Recognition of Electronic Records & Signatures

- Electronic records (like PDF contracts, scanned documents) and **electronic signatures/digital signatures** are now given **legal recognition** in India.
- This means online communication and agreements are **legally valid**.
- **Example:** If a company signs a business contract with a **digital signature**, it is legally binding like a handwritten signature.
- The **Indian Institutes of Information Technology Laws (Amendment) Bill, 2020** further strengthened protection for **electronic records and signatures**, ensuring organizations get full **legal support** in digital transactions.

4.9 Cybercrime and Punishment

Why cybercrime is different from normal (physical) crime?

1. **Easy to learn** – Anyone with basic skills can learn how to hack, phish, or commit fraud.
   - Example: A student can learn phishing techniques from YouTube and trick people.
2. **Fewer resources needed** – A single computer + internet can cause damage worth millions.
   - Example: One hacker can steal thousands of credit card numbers using malware.
3. **No need to be physically present** – You can commit a cybercrime in another country while sitting at home.
   - Example: A hacker in India can steal money from US bank accounts without visiting the US.
4. **Not always clearly illegal** – Some activities (like scanning websites for vulnerabilities) may not be clearly covered under old laws.

Challenges in Punishing Cybercriminals

- Some countries don't have **clear cybercrime laws**.
- Police often treat cybercrime like traditional crime, which causes confusion.
- Example: In the early days, a **DDoS attack** on an e-commerce site wasn't seen as "damage to property" because digital property wasn't recognized by old laws.

Key Points on Cybercrime Punishment

1. **Relying only on traditional laws is not enough** – Old laws can't handle modern cybercrimes.
2. **Weak penalties** – Small punishments don't scare cybercriminals.
3. **Self-protection is key** – Companies and individuals must secure themselves first.
    - Example: Using antivirus, firewalls, and two-factor authentication.
4. **Different laws in different countries** – Creates confusion in international cases.
    - Example: What is illegal in India may not be illegal in another country.
5. **Need for a model approach** – A unified system across countries is required.

 Solution suggested:
A **public-private partnership** (government + private companies) to create a **global model cyber law** to deal with crimes effectively.

4.10 Cyberlaw, Technology, and Students: Indian Scenario

- In India, there is a **knowledge gap**:
    - **Tech students** (BCA, B.Tech, MCA) → know computers but don't know **cyberlaw**.
    - **Law students** → know laws but don't understand **technology deeply**.

 This gap makes it difficult to handle **cybercrimes legally**, since both technical and legal knowledge are required.

- **Example:**
    - A BCA student may know how hacking happens but not what sections of IT Act apply.
    - A law student may know ITA 2000 provisions but not understand how a DDoS attack works.

4.21 Cybercrimes and Cyber Security: The Legal Perspectives

1. **Computer Science students' limitation**

- In some colleges, Computer Science students learn how to create programs that send data across the internet (using TCP/IP packets).
- But they are **not taught about the dangers**, like hacking or spreading viruses.
- Example: A student may learn to write a program that sends files automatically, but may not realize it could also be misused for data theft.

2. **Lack of Secure Coding in Education**
   - Most universities do **not teach secure coding**.
   - This means students may unknowingly write programs that have **security holes**, making them easy targets for hackers.
3. **Law Students' limitation**
   - Law students are taught about **trademark and copyright laws**, but not how these apply to **electronic/digital content**.
   - Example: They know plagiarism in books is wrong, but may not fully understand copyright violations on digital files, music, or software.
4. **Knowledge Gap**
   - As a result:
     - Technologists (engineers, programmers) → don't understand cyber laws.
     - Lawyers → don't understand technology.
   - This gap makes it harder to fight cybercrime effectively.
5. **What should be done in the future?**
   - **Engineering, Commerce, and Management colleges** → must include **Cyber Law** in their syllabus.
   - **Law colleges** → must expand their teaching to include **cybercrime laws and intellectual property rights (IPR) in digital space**.