UNIT-I
Introduction

Introduction: History of Internet and World Wide Web, Need for cyber law, Cybercrime on the rise, Important terms related to cyber law. Cyber law in India: Need for cyber law in India, History of cyber law in India, Information Technology Act, 2000, Overview of other laws amended by the IT Act, 2000, National Policy on Information Technology 2012.

History of Internet and World Wide Web:

The history of the Internet is a story of innovation, collaboration, and technological evolution. Here's a concise overview of the key developments:

1. Pre-Internet Foundations (1950s–1960s)
   - Cold War Influence: The U.S. government wanted a communication system that could survive a nuclear attack.
   - Packet Switching: Invented independently by Paul Baran (RAND Corporation, USA) and Donald Davies (NPL, UK). This broke data into packets for transmission.
   - Time-Sharing Systems: Early multi-user systems developed in institutions like MIT laid groundwork for online computing.

2. ARPANET: The Birth of the Internet (1969)
   - ARPANET (Advanced Research Projects Agency Network): First packet-switching network, funded by the U.S. Department of Defense.
   - First Message Sent: October 29, 1969, between UCLA and Stanford; the system crashed after the second letter.
   - Email: Introduced in 1971 by Ray Tomlinson—the first use of the "@" symbol in addresses.

3. Protocol Development (1970s–1980s)
   - TCP/IP Protocols (1974–1983): Developed by Vint Cerf and Bob Kahn. These standardized rules for communication between networks.
   - ARPANET switches to TCP/IP: On January 1, 1983—this date is considered the birth of the "modern Internet."
   - Domain Name System (DNS): Introduced in 1984, replacing IP addresses with easier-to-remember domain names like .com, .edu, .gov.

4. Expansion and the Rise of the Web (1980s–1990s)
   - NSFNET (National Science Foundation Network): Replaced ARPANET and connected more universities and institutions.
   - Commercial Use Begins: Restrictions on commercial use were lifted in the late 1980s.
   - World Wide Web (WWW): Invented in 1989 by Tim Berners-Lee at CERN. Introduced the concept of websites and hyperlinks.
   - First Web Browser (1993): Mosaic, later evolved into Netscape.

5. Internet Boom and Global Adoption (1990s–2000s)
   - Dot-com Boom (mid-1990s to 2000): Surge in tech startups and online businesses.

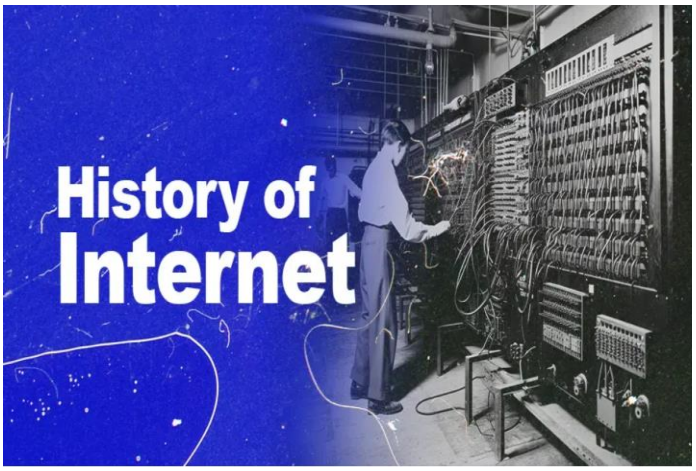
- Broadband Expansion: Faster home internet access increased multimedia use.

- Search Engines: Yahoo (1994), Google (1998) changed information access.
- Social Media Begins: Friendster (2002), MySpace (2003), Facebook (2004).

6. Mobile and Social Era (2010s–Present)
   - Smartphones and Apps: Widespread mobile internet access with iPhone (2007) and Android (2008).
   - Cloud Computing: Services like Google Drive, AWS revolutionize storage and services.
   - Streaming and IoT: Netflix, YouTube, Spotify, and smart home devices expand use cases.

7. Current Trends and Future Outlook

- AI & Machine Learning: Power modern search engines, recommendation systems, and automation.
- 5G Networks: Enabling faster, low-latency connections.
- Decentralization & Web3: Blockchain-based systems and cryptocurrencies propose alternatives to traditional centralized internet services.



World Wide Web:

The World Wide Web (WWW), often called the Web, is a system of interconnected webpages and information that you can access using the Internet. It was created to help people share and find information easily, using links that connect different pages together. The Web allows us to browse websites, watch videos, shop online, and connect with others around the world through our computers and phones.

All public websites or web pages that people may access on their local computers and other devices through the internet are collectively known as the World Wide Web or W3. Users can get further information by navigating to links interconnecting these pages and documents. This data may be presented in text, picture, audio, or video formats on the internet.

Fact: Today, it connects over 63% of the world's population, making it one of the most powerful tools for communication and information sharing.

Key Parts of the Web

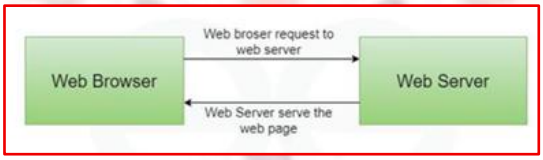
The Web has three main building blocks that make it work:

- URL (Uniform Resource Locator): This is the address of a webpage, like https://www.example.com. It tells your browser exactly where to find the page.
- HTTP (Hypertext Transfer Protocol): This is the set of rules that lets your browser and the server talk to each other to send and receive webpages.
- HTML (Hypertext Markup Language): This is the code that tells browsers how to display a webpage, including where to put text, pictures, and links.

Working of World Wide Web(WWW)

A Web browser is used to access web pages. Web browsers can be defined as programs which display text, data, pictures, animation and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interfaces provided by Web browsers. Initially, Web browsers were used only for surfing the Web but now they have become more universal.

The below diagram indicates how the Web operates just like client-server architecture of the internet. When users request web pages or other information, then the web browser of your system request to the server for the information and then the web server provide requested services to web browser back and finally the requested service is utilized by the user who made the request.



Web browsers can be used for several tasks, including conducting searches, mailing, transferring files, and much more. Some of the commonly used browsers are Internet Explorer, Opera Mini, and Google Chrome.

Challenges of the Web

The Web is amazing, but it has some problems that you should know about:

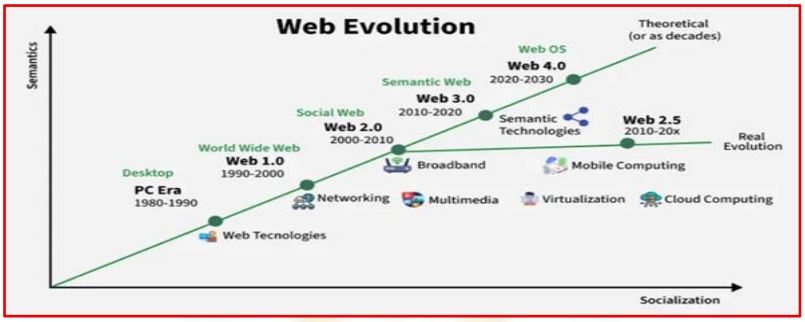
- **Privacy**: Some websites collect information about you, like what you search for, and might share it without asking.
- **Safety**: Hackers can try to steal your information or send viruses through fake links or ads.
- **False Information**: Not everything on the Web is true, so you need to check if a website is trustworthy.
- **Bullying**: Some people use the Web to be mean or bully others, which can hurt feelings.
- **Too Much Screen Time**: Spending too much time online can make it hard to focus on school or sleep well.
- **Access Issues**: Not everyone has fast Internet, especially in some countries, which makes it harder to use the Web.

History of the WWW

It is a project created, by Tim Berner Lee in 1989, for researchers to work together effectively at CERN. It is an organization, named the World Wide Web Consortium (W3C), which was developed for further

development of the web. This organization is directed by Tim Berner's Lee, aka the father of the web. CERN, where Tim Berners worked, is a community of more than 1700 researchers from more than 100 countries. These researchers spend a little time on CERN and the rest of the time they work at their colleges and national research facilities in their home country, so there was a requirement for solid communication so that they can exchange data.

How Web Evolves?



World Wide Web(WWW) Evolved so much from web 1.0 to web 4.0 (Future of WWW) as follows:

- Web 1.0 (1990–2000) Introduced static websites,
- while Web 2.0 (2000–2010) brought interactive and social platforms.
- Web 3.0 (2010–2020) focused on the semantic web, enabling machines to understand data and offer personalized experiences.
- Looking ahead, Web 4.0 (2020–2030) is expected to be a fully intelligent web ecosystem powered by AI and integrated web operating systems.

Some Facts About the Web

- The first website ever is still online! You can visit it at "**http://info.cern.ch**"
- There are over 1.5 billion websites in the world, and that number grows every day.
- Google Chrome is used by more than 60% of people browsing the Web.
- The Web is available in over 150 languages, so you can explore in your language or learn a new one!

World Wide Web (WWW) Vs Internet

It's easy to mix up the Web and the Internet, but they're different:

Aspect	World Wide Web	Internet
What It Is	A collection of webpages and websites you access with a browser.	A global network connecting computers.
Started	1989 by Tim Berners-Lee at CERN.	1960s as ARPANET.
Purpose	To share and explore information like text, images, and videos.	To connect devices and share data.
How You Use It	Through browsers like Chrome or Firefox.	Through any connected device for email, apps, etc.
Example	Visiting a website like Wikipedia.	Sending an email or streaming a video.

Need for Cyber Law:

Cyberlaw is the law of handling issues related to the digital world. It protects from cyber-attacks and is aware of future attacks. In this article, we will cover a brief explanation of cyber law and its importance of cyberlaw.

What is Cyber Law?

Cyberlaw is the safeguard from the digital world. It stops illegal activity on the internet such as hacking, online harassment, etc. It helps to protect persons or businesses from cybercriminal activity. Cyberlaw provides the prevention measures that users read before using the internet and doing online business because this helps users to protect from cyber-criminal activities and protect from unauthorized activities. The first cyber law i.e. Computer Fraud and Abuse Act was introduced in 1986 which prevents unauthorized users and gives punishment for breaking the laws.

Types of Cyberlaw

Here are the types of Cyberlaw-

- **Privacy laws:-** Privacy laws protect the personal or sensitive information of persons or businesses that are present online.
- **Intellectual property laws:-** It protects the digital content that is posted online. For Example, you upload a video and someone steals your video and posts it on YouTube by your name in that case, these laws stop and prevent copyright. If anyone copies the content, this law automatically removes the content and gives restrictions to the copied user.
- **Data protection laws:-** It is the backbone of users to protect their personal information and to protect them from hacker attacks or third-party misuse of the data.
- **Cyber Crime laws:-** The main focus of this law is to monitor criminal or illegal activity that goes online or internet such as hacking, credit card fraud, and online fraud. These laws take strict action from the hackers or persons who do these illegal activities.
- **Cyber security laws:-** These laws help to protect organizations from malicious threats. It provides various security measures that recover organizations or businesses from cyber attacks.
- **Ecommerce laws:-** E-commerce laws indicate online transactions and electronic signatures. The law is set by an e-commerce company. This law acts as a safeguard for users to protect from fraudulent activity and provides security in online transactions. E-commerce platforms such as Amazon, and Flipkart where many users select online transactions to pay for products, and e-commerce laws make sure the online transaction is securely done by users and protect their sensitive information.
- **Computer crime laws: -** These laws protect users from unauthorized access to computer systems and protect them from phishing attacks. The focus of this law is to stop the illegal activity that is done by computer systems and take strict actions.
- **Social media laws: -** It protects us from social media activity such as harmful content, online harassment, and negative comments. for ex- If someone posts content on social media but the content hurts the audience in that case social media and online content regulation laws remove the content and give restrictions or claims for these types of content.
- **Cryptocurrency regulations: -** This law protects from cryptocurrency trading issues. Depending upon the regulations in different countries, some countries ban cryptocurrency.

Objectives of Cyber Law

Here are the objectives of Cyberlaws:-

- It protects from malicious threats and online data threats.
- It protects from online fraudulent transactions.
- It protects our sensitive data or business data.
- It takes strict actions or punishment for the individuals who do wrong things in the digital world.
- It blocks unknown or unusual transactions.
- Cyberlaw ensures trust between all the users to secure them from unauthorized access.

Importance of Cyber Law

Here are the importance of Cyber Law-

- It increases safety while making online transactions.

It solved the issues related to cybercrime.

- All the organization safely stored the data in electronic form.
- It enhances the national security.
- It also prevents from misuse of computers and any electronic devices.
- It protects the user's sensitive information and prevents any attacks.
- It allows all the employees to work safely in a remote environment.

Challenges of Cyber Law

Here are the challenges of Cybe Law-

- The first challenge of Cyberlaw is to mobile laws. There are no regulations for mobile devices and tablets. Many Criminal activities are involved in mobile devices and there the some challenges that the cyber legal to investigate the device. The solution to this is to focus on more mobile devices as well so that people securely use mobile devices without the fear of cyber attacks.
- The second challenge is cloud computing. Our data is stored in cloud storage. Cyber law makers face some issues related to data privacy and data security.

Significance of Cyber Law

Cyber law is crucial for several reasons:

- **Safeguarding Security:** It sets norms for how individual data ought to be dealt with, guaranteeing people's information is shielded from unapproved access and abuse.
- **Managing Cybercrime:** Digital regulations characterize and punish different types of cybercrime, for example, hacking, data fraud, and online misrepresentation, making it simpler to arraign guilty parties.
- **Laying out Web-based Direct Principles:** These regulations help in establishing a protected and conscious internet-based climate by controlling ways of behaving like provocation, criticism, and protected innovation robbery.
- **Supporting Internet business:** They give a legal system to online exchanges, contracts, and computerized marks, which is fundamental for the development of internet business and online organizations.
- **Guaranteeing Consistence:** Organizations need to conform to digital regulations to keep away from legitimate punishments and keep up with customer trust, which is fundamental for functional steadiness and notoriety.

- **Worldwide Participation:** Digital regulations work with worldwide collaboration in handling cross-line cybercrime and safeguarding worldwide data frameworks.
- **Advancing Security:** They expect associations to execute safety efforts to safeguard information and frameworks, which generally improve network protection.
- **Empowering Development:** By laying out clear, legitimate rules, digital regulation can assist with cultivating advancement while adjusting the requirements for insurance and guidelines.

Advantages of Cyber Law

Cyber law offers several advantages:

- **Improved Security:** Gives legitimate measures to safeguard against digital dangers, guaranteeing that the two people and associations can defend their advanced resources.
- **Security Insurance:** Lays out rules for dealing with individual data, which forestall abuse and unapproved access, in this manner safeguarding people's protection.
- **Prevention of Cybercrime:** By characterizing and punishing unlawful internet-based exercises, digital regulations hinder possible wrongdoers and decrease the commonness of cybercrime.
- **Lawful Lucidity:** Offers clear rules and norms for computerized collaborations, diminishing vulnerability and assisting people and organizations with figuring out their freedoms as well as certain limitations.
- **Purchaser Security:** Guarantees that organizations stick to norms that safeguard customers from misrepresentation, tricks, and information breaks, cultivating trust in web-based exchanges.
- **Guidelines for Web-Based Business:** Works with secure and legitimate web-based exchanges by perceiving computerized agreements and marks, which upholds the development of web-based business.
- **Worldwide Participation:** Elevates cooperation between nations to address cross-line digital issues, working on worldwide network safety and policing.

Cyber Crime on the Rise:

"Cybercrime is indeed on the rise, with significant financial and societal impacts projected for the coming years. It's evolving rapidly, driven by increasingly sophisticated tactics and the widespread availability of new technologies, particularly Artificial Intelligence (AI).

Key Statistics and Projections:

- **Massive Financial Cost:** Cybercrime damages are projected to reach an astounding **$10.5 trillion annually by the end of 2025**, making it comparable to the world's third-largest economy if it were a country (behind only the U.S. and China). This is a substantial increase from $3 trillion in 2015.
- **Rising Data Breach Costs:** The average cost of a data breach globally increased to **$4.88 million in 2024**, a 10% rise from the previous year, highlighting the growing financial burden on organizations.
- **Increased Attack Frequency:** The average number of cyberattacks per organization per year has increased by 25%, from three to four.

Major Trends and Types of Cybercrime on the Rise:

1. **AI-Driven Attacks:** This is a critical and accelerating trend.
    - **Sophistication and Scale:** Cybercriminals are using AI to automate complex attacks,

making them more efficient, harder to detect, and scalable. AI can quickly identify software flaws, modify AI models, and reconstruct training data.

- **Advanced Phishing and Social Engineering:** Generative AI (GenAI) is supercharging phishing and social engineering attacks, making them far more convincing and personalized. This includes AI-generated emails, websites, and even deepfakes (fake videos and audio) used for impersonation and disinformation.
- **Lowering Barriers to Entry:** AI tools, especially Large Language Models (LLMs), are enabling individuals with limited technical skills to launch sophisticated attacks.
- **AI Agents for Malware and Reconnaissance:** Experts predict the rise of autonomous AI agents that can perform tasks like scanning networks, extracting passwords, and even collaborating on attacks.

2. **Ransomware:** Continues to be a dominant and costly threat.
   - **Significant Damages:** Global ransomware damages are expected to reach **$57 billion in 2025**, breaking down to approximately $6.5 million per hour.
   - **Targeted Attacks:** Ransomware attacks are increasingly targeted, with industries like healthcare and manufacturing being particularly vulnerable. In 2024, data breaches involving healthcare organizations increased by 25%.
3. **Supply Chain Attacks:** Cybercriminals are increasingly targeting supply chains to compromise multiple organizations through a single breach. This risk is amplified by the growing complexity and lack of visibility into supplier security.
4. **Cloud Security Vulnerabilities:** While cloud providers offer robust security, user-end errors, malicious software, and phishing attacks continue to create vulnerabilities in cloud environments. Cloud intrusions increased by 75% in 2023.
5. **Internet of Things (IoT) Vulnerabilities:** The proliferation of IoT devices creates a wider attack surface. Many IoT devices lack strong security features, making them easy targets for exploitation.
6. **Cybercrime-as-a-Service (CaaS):** The dark web offers various tools and services for cyberattacks, allowing even lower-skilled individuals to launch complex attacks.
7. **Deepfake Technology Exploitation:** The misuse of deepfake technology for impersonation, financial fraud, and reputational damage is a growing concern.

Factors Contributing to the Rise:

- **Digital Transformation:** Increased reliance on digital platforms for business, government, and personal activities creates more opportunities for cybercriminals.
- **Sophisticated Attack Techniques:** Cybercriminals are constantly innovating and developing new methods.
- **Cybersecurity Skills Gap:** There's a persistent shortage of qualified cybersecurity professionals, leaving many organizations vulnerable.
- **Geopolitical Tensions:** Geopolitical turmoil is influencing cybersecurity strategies, with an increase in cyber espionage and attacks targeting critical infrastructure.

Combating the Trend:

To counter the rising tide of cybercrime, organizations and individuals need to prioritize cybersecurity. This includes:

- **Increased Investment:** Global spending on cybersecurity products and services is projected to reach $1.75 trillion cumulatively from 2021 to 2025.
- **Robust Security Measures:** Implementing advanced security solutions, including AI-based defensive tools, multi-factor authentication (MFA), and Zero Trust architectures.
- **Employee Training and Awareness:** Educating users about the latest phishing techniques, social engineering tactics, and general cybersecurity best practices.
- **Proactive Threat Intelligence:** Staying informed about emerging threats and adversary tactics.
- **Incident Response and Recovery Planning:** Having well-defined plans to respond to and recover from cyber incidents.
- **Secure IoT Devices:** Changing default passwords, regularly updating firmware, and segmenting IoT devices on separate networks.
- **Focus on Supply Chain Security:** Ensuring the security posture of third-party vendors and suppliers.

The fight against cybercrime is a continuous and evolving battle, requiring constant vigilance and adaptation from all stakeholders."

Important Terms Related to Cyberlaw:

- **Cyberlaw:** The area of law that deals with the Internet, computer systems, and digital communications. Also known as Internet Law or IT Law.
- **Cybercrime:** Criminal activities carried out using computers or the internet, such as hacking, identity theft, and cyberstalking.
- **Data Protection:** Legal control over access to and use of data stored in computers. Ensures privacy of individuals' personal data.
- **Digital Signature:** An encrypted signature used to authenticate the origin and integrity of digital messages or documents.
- **Hacking:** Unauthorized access to or manipulation of computer systems or networks.
- **Phishing:** A form of online fraud where attackers impersonate legitimate institutions to steal sensitive information.
- **Malware:** Malicious software designed to disrupt, damage, or gain unauthorized access to a computer system.
- **Intellectual Property Rights (IPR):** Legal rights protecting creations of the mind (e.g., software, logos, digital media) under copyright, patents, or trademarks.
- **Information Technology Act, 2000 (India): T**he primary law in India dealing with cybercrime and electronic commerce.
- **E-commerce Law:** Laws that govern electronic transactions, digital contracts, and online business activities.
- **Cybersecurity:** The practice of protecting systems, networks, and data from digital attacks.
- **Spam:** Unsolicited electronic messages, often sent in bulk, usually for advertising.
- **Identity Theft:** Fraudulent acquisition and use of someone's personal information, often for financial gain:
- **Computer Forensics:** The process of collecting, analyzing, and presenting digital evidence in a legal context.

- **Jurisdiction in Cyberspace:** The authority of courts to rule over legal disputes involving online activities that may cross territorial boundaries.

Cyberlaw in India

Need for Cyberlaw in India:

The need for **cyber law in India** is critical due to the growing dependence on digital technology, internet-based transactions, and the proliferation of cybercrimes. Here's a concise breakdown of the **reasons cyber law is essential in India**:

1. Rise in Cybercrimes

- India has seen a steep increase in cybercrimes like hacking, identity theft, cyberstalking, phishing, and ransomware attacks.
- Cyber law provides a legal framework to investigate, prosecute, and penalize cybercriminals.

2. Growth of E-commerce and Digital Payments

- With the rise of platforms like UPI, Paytm, and online banking, there's a greater risk of online fraud.
- Cyber law ensures secure digital transactions and helps resolve disputes between consumers and service providers.

3. Protection of Personal Data

- Individuals' data is vulnerable to misuse in the digital space.
- Cyber laws help protect privacy and ensure that companies handle data responsibly (e.g., the **Digital Personal Data Protection Act, 2023**).

4. Legal Recognition of Electronic Records

- Under the **Information Technology Act, 2000**, electronic records and digital signatures are legally valid.
- This is essential for online contracts, e-governance, and paperless documentation.

5. Regulation of Cyber Activities

- Cyber law defines what constitutes a cyber offense and regulates behavior online.
- It helps curb illegal content, software piracy, cyberbullying, and misinformation.

6. National Security Concerns

- Cyberattacks can target critical infrastructure like power grids, banking systems, and defence.
- Cyber law helps in building a robust cybersecurity framework and addressing cyberterrorism.

Key Cyber Law in India

- **Information Technology Act, 2000 (IT Act)**: Main legislation for cyber law in India.
  - Amended in 2008 to cover data protection, cyber terrorism, and intermediary liability.

History of Cyber Law in India:

With the rise of the internet and digital technologies, India recognized the need for laws to regulate cyberspace. Cyber laws in India have evolved to address issues like **cybercrime, data protection, e-commerce, and digital privacy**. The **Information Technology (IT) Act, 2000** is the primary law governing cyber activities in India.

Early Developments (Before 2000)

A. Lack of Cyber Laws in the 1990s

- Before 2000, there were no specific laws to regulate digital crimes or online activities in India.
- Cybercrimes like hacking, online fraud, and identity theft were increasing, but existing laws (such as the **Indian Penal Code, 1860**) were insufficient to handle them.
- The rapid growth of the **IT industry and e-commerce** created a demand for legal regulations.

B. Influence of International Laws

- India was influenced by the **UNCITRAL** Model Law on Electronic Commerce (1996**)**, which provided guidelines for electronic contracts and digital signatures.
- The need to comply with international standards led to the formation of cyber laws in India.

Enactment of the IT Act, 2000

A. Introduction of the Information Technology (IT) Act, 2000

- The **IT Act, 2000** was enacted on **October 17, 2000**, to provide a legal framework for electronic governance, cybercrimes, and digital transactions.
- It **recognized electronic records and digital signatures**, making online contracts legally valid.

B. Key Provisions of the IT Act, 2000

- **Legal recognition of electronic documents** – Digital documents were accepted as legal evidence.
- **Digital signatures** – Provided security for online transactions.
- **Cybercrime laws** – Punished hacking, identity theft, phishing, and online fraud.
- **Regulation of cybercafés and online businesses** – Ensured monitoring of cyber activities.

Amendments and Evolution of Cyber Law

A. IT (Amendment) Act, 2008

- The **IT Act, 2000** was amended in **2008** to address emerging cyber threats like **cyber terrorism, data breaches, and identity theft**.
- **Key Changes:**
    1. **Section 66A** – Criminalized sending offensive or false messages via electronic means (later struck down in 2015).
    2. **Section 66B, 66C, 66D** – Introduced strict punishments for identity theft, online fraud, and impersonation.
    3. **Section 69** – Gave the government power to intercept, monitor, and decrypt information for national security.
    4. **Section 72A** – Punished the disclosure of personal information without consent.

B. Landmark Cases Leading to Cyber Law Reforms

- **Shreya Singhal v. Union of India (2015)** – **Section 66A was struck down** for violating free speech rights.
- **Aadhaar Data Privacy Case (2017)** – Supreme Court ruled **privacy as a fundamental right**, influencing data protection laws.

C. Personal Data Protection Bill (PDPB), 2019

- Inspired by **Europe's GDPR**, this bill aimed to regulate data collection, processing, and storage.

- It proposed **strict rules for companies handling user data** and penalties for data misuse.
- However, it was later replaced by the **Digital Personal Data Protection Act, 2023**.

D. **Digital Personal Data Protection Act (DPDP), 2023**

- Passed to **protect individual privacy and regulate personal data usage**.
- Key features:
  - Companies must obtain **user consent** before collecting data.
  - Users have the right to **access, correct, and erase personal data**.
  - Heavy **penalties for data breaches** and non-compliance.

Challenges in Cyber Law Implementation

- **Cross-border cybercrimes** – Many cybercriminals operate from different countries, making it difficult to enforce laws.
- **Lack of awareness** – Many people and businesses are unaware of cyber laws and security practices.
- **Need for stronger enforcement** – Many cybercrimes go unreported, and law enforcement lacks technical expertise.
- **Emerging threats** – Cyber laws must continuously evolve to address AI-driven fraud, deepfake technology, and blockchain-related crimes.

Future of Cyber Law in India

- **Stronger Data Protection Laws** – India may introduce stricter laws like **GDPR** to regulate data privacy.
- **Regulation of Artificial Intelligence (AI)** – Laws may be needed to prevent misuse of AI in cybercrimes.
- **Better Cybercrime Investigation** – More investment in cybersecurity training and technology.

International Cooperation – India must collaborate with global agencies to combat cross-border cyber threat

Information Technology (IT) Act, 2000

Information Technology (IT) Act, 2000:

The **Information Technology (IT) Act, 2000** was India's first cyber law, enacted to regulate **electronic commerce, digital transactions, cybercrime, and online security**. It provides a legal framework for the recognition of **electronic records, digital signatures, and penalties for cyber offenses**. The Act has undergone amendments, particularly in **2008**, to address emerging cyber threats.

1. Legal Recognition of Electronic Records & Digital Signatures

- **Electronic documents** are considered legally valid, just like paper-based records.
- **Digital signatures** (now replaced with electronic signatures) are legally recognized for authentication of electronic documents

2. Cybercrimes and Penalties

The IT Act defines **various cybercrimes** and prescribes penalties:

- **Hacking (Section 66)** – Unauthorized access to computer systems is punishable with

imprisonment up to **3 years** or a fine up to **₹5 lakh**.

- **Identity Theft (Section 66C)** – Using someone's personal information (passwords, biometric data) is punishable with **3 years of imprisonment** and a fine.
- **Cheating by Personation (Section 66D)** – Fraud through online impersonation is punishable with **3 years' imprisonment** and a fine.

- **Publishing Obscene Content (Section 67)** – Sharing sexually explicit content online can lead to **up to 5 years in jail and a fine of ₹10 lakh**.
- **Cyber Terrorism (Section 66F)** – Acts that threaten national security using computers or networks are punishable with **life imprisonment**.

3. Government's Power to Monitor & Intercept Data

- **Section 69** – The government can **intercept, monitor, or decrypt** any information for national security, public order, or to prevent cyber threats.
- **Section 69A** – Grants the power to **block websites** in the interest of national security (e.g., banning of Chinese apps like TikTok).
- **Section 69B** – Allows government agencies to **monitor and collect traffic data** for cybersecurity purposes.

4. Liability of Network Service Providers (ISPs & Intermediaries)

- **Section 79** – Intermediaries (such as social media platforms, ISPs) are not liable for third-party content **if they follow due diligence** and remove illegal content when notified.

5. Recent rules (IT Rules, 2021) – Mandated platforms like WhatsApp, Facebook, and Twitter to appoint **grievance officers** and comply with stricter regulations.**Recognition of Electronic Governance**

- **Section 4** – Government agencies must accept electronic documents and records.
  Section 6 – Electronic contracts and digital records have the same legal standing as traditional paper documents.

6. Cybersecurity & Data Protection

- **Section 43** – Unauthorized access, data theft, or introducing viruses into a computer system results in liability for damages up to **₹1 crore**.
- **Section 72A** – Disclosure of personal information without consent leads to **imprisonment for 3 years or a fine of ₹5 lakh**.

7. mendments & Developments

- **IT (Amendment) Act, 2008** – Added **cyber terrorism laws, identity theft provisions, and stronger penalties for cybercrimes**.
- **Section 66A (Struck Down in 2015)** – Originally punished sending offensive messages online but was declared unconstitutional in **Shreya Singhal v. Union of India**.
- **Personal Data Protection Bill (2019) & Digital Personal Data Protection Act (2023)** – Introduced stricter rules for handling personal data.

National Policy on Information Technology (NPIT) 2012

Introduction:

The **National Policy on Information Technology (NPIT) 2012** was introduced by the Government of India to promote the growth of the **Information Technology (IT) and Information Technology Enabled Services (ITES) sector**. The policy aimed to increase IT's contribution to **economic growth, job creation, and digital infrastructure development** while ensuring cybersecurity and innovation.

Objectives of NPIT 2012:

The key objectives of the **NPIT 2012** were:

- **Increase IT's contribution to GDP** from around 7.5% (in 2012) to **more than 10%**.
- **Create 10 million IT jobs** to boost employment in the sector.
- **Promote IT innovation** by supporting research and development (R&D).
- **Develop a secure cyber ecosystem** to strengthen cybersecurity.
- **Expand e-Governance services** for better public service delivery.
- **Encourage investment in IT and ITES sectors** to attract global companies.
- **Enhance digital literacy** and promote IT education.

Key Features of NPIT 2012:

A. Growth of IT and IT-Enabled Services (ITES)

- Encouraged **expansion of IT industries in Tier 2 and Tier 3 cities**.
- Promoted **Foreign Direct Investment (FDI) in IT & ITES**.
- Focused on increasing India's **software exports**.

B. Promotion of Research and Innovation

- **Encouraged R&D** in emerging technologies like **cloud computing, artificial intelligence (AI), and cybersecurity**.
- Supported **startups and entrepreneurs** in the IT sector.

C. Development of a Secure Cyber Ecosystem

- Strengthened cybersecurity frameworks to prevent **cyber threats and hacking**.
- Promoted awareness programs for **safe and responsible use of IT**.

D. Expansion of e-Governance Services

- Encouraged **digitalization of government services** to improve transparency.
- Focused on **Aadhaar-linked services** and digital payments.

E. IT for Inclusive Growth

- Promoted IT education and skill development to **bridge the digital divide**.
- Encouraged IT adoption in **healthcare, agriculture, and education**.

F. Open Standards and Interoperability

- Ensured government IT systems follow **open standards** for easy data sharing.
- Promoted the use of **free and open-source software (FOSS)**.

Impact of NPIT 2012 <u>Positive Outcomes</u>

✅ **Boosted IT Industry Growth** – Helped increase software exports and IT-enabled services.

✅ **Expanded Digital India Initiative** – Strengthened e-Governance services.

✅ **Improved Cybersecurity Policies** – Led to stronger cybersecurity frameworks.

Challenges and Limitations

❌ **Lack of strong data protection laws** – The Personal Data Protection Bill (PDPB) was delayed.

❌ **Slow infrastructure development** – Digital connectivity in rural areas remained a challenge.

❌ **Cybersecurity risks increased** – Despite policies, cyber threats continued to grow.

UNIT-II

Overview Of The Information Technology Act, 2000: Applicability of the Act, Important provisions of the Act: Digital signature and Electronic signature, Digital Signature under the IT Act, 2000, EGovernance Attribution, Acknowledgement and Dispatch of Electronic Records, Certifying Authorities, Electronic Signature Certificates, Duties of Subscribers, Penalties and Offences, Intermediaries.

Applicability of the Act:

The **Information Technology Act, 2000 (IT Act)**, as amended, is the primary legislation in India dealing with various aspects of the digital and electronic realm. Its applicability is broad and far-reaching, designed to provide a legal framework for electronic transactions, prevent cybercrime, and facilitate e-governance.

Here's a breakdown of the applicability of the IT Act:

I. Territorial Applicability

1. **Whole of India:** The Act extends to the whole of India. This means its provisions are binding across all states and Union Territories within the country.
2. **Extraterritorial Jurisdiction (Section 75):** This is a crucial aspect of the IT Act's applicability. It states that the Act also applies to:
    - **Any offense or contravention committed outside India**
    - **By any person (irrespective of their nationality)**
    - **Provided such offense or contravention involves a computer, computer system, or computer network located in India.**

Example: If a hacker in another country uses a server located in India to launch a cyberattack on a company in the USA, or if a person in the UK uses an Indian server to spread defamatory content about someone in India, they can be prosecuted under the Indian IT Act. This broad reach is essential for dealing with the borderless nature of cybercrime.

II. Subject Matter Applicability

The IT Act applies to and provides legal recognition for a wide range of electronic activities and digital assets:

1. **Electronic Records:**
    - It gives legal validity to information in electronic form, ensuring that electronic documents, data, and communications (like emails, messages, digital files) are treated as legally equivalent to their paper-based counterparts (Section 4).
    - This is fundamental for e-commerce, e-governance, and digital evidence in court.

2. **Electronic Signatures (including Digital Signatures):**
    - The Act provides legal recognition to electronic signatures affixed to electronic records, making them legally binding (Section 5, 3A). This facilitates secure online authentication and contracting.
    - It also lays down the framework for Certifying Authorities (CAs) and the issuance of Digital Signature Certificates (DSCs).
3. **E-Governance:**
    - It facilitates and promotes electronic governance by enabling government agencies to accept, file, and retain documents, issue licenses, collect payments, and provide services electronically (Sections 6, 6A, 7, 8).
4. **Electronic Commerce (E-commerce):**
    - The Act provides the legal basis for conducting transactions electronically, ensuring the validity of electronic contracts (Section 10A) and secure communication for commercial purposes.
5. **Cybercrimes:**
    - A significant portion of the Act is dedicated to defining various cybercrimes and prescribing penalties for them. This includes:
        - Hacking and unauthorized access (Section 43, 66)
        - Identity theft and cheating by personation (Sections 66C, 66D)
        - Violation of privacy/revenge pornography (Section 66E)
        - Cyber terrorism (Section 66F)
        - Publishing/transmitting obscene or explicit material (Sections 67, 67A, 67B - including child pornography)
        - Data theft and breach of confidentiality (Section 72, 72A)
6. **Intermediary Liability:**
    - It defines the role and liabilities of intermediaries (like social media platforms, internet service providers, telecom service providers) and provides conditions under which they can be exempted from liability for user-generated content (Section 79). This aspect has been further detailed by the Intermediary Guidelines Rules, 2021.
7. **Cyber Security & Regulation:**
    - Establishes authorities like the Controller of Certifying Authorities (CCA) to regulate digital signatures.

- Empowers the government to monitor, intercept, or block information in cyberspace under specific conditions (Sections 69, 69A).
- Recognizes bodies like CERT-In (Indian Computer Emergency Response Team) for cyber security incident response.

8. **Data Protection (Historically):**
   - Prior to the Digital Personal Data Protection Act, 2023, Section 43A and the SPDI Rules, 2011, under the IT Act, served as the primary framework for data protection, especially for sensitive personal data handled by body corporates. While the DPDP Act is now the overarching data protection law, the IT Act still has provisions related to data integrity and security in other contexts.

III. Non-Applicability (Documents Excluded from Electronic Form)

Despite its broad applicability, Section 1(4) and the First Schedule of the IT Act explicitly state that it does *not* apply to certain documents or transactions, which still require physical form for legal validity:

- **Negotiable Instruments (other than a cheque):** Bills of exchange, promissory notes. Cheques are included as they are typically processed electronically.
- **Powers of Attorney:** Documents granting authority to another person to act on one's behalf.
- **Trusts:** Documents creating or dealing with trusts.
- **Wills and any other Testamentary Disposition:** Documents related to inheritance and succession after death.
- **Any contract for the sale or conveyance of immovable property or any interest in such property:** While preliminary agreements might be electronic, the final conveyance and registration of immovable property usually require physical documents and registration with the appropriate authorities.

Digital signature and Electronic signature:

In India, both "Digital Signature" and "Electronic Signature" are legally recognized under the **Information Technology Act, 2000 (IT Act)**, but they represent different levels of security and specific technological implementations. While all Digital Signatures are a type of Electronic Signature, not all Electronic Signatures are Digital Signatures.

Let's break down the definitions and key differences in the Indian context:

1. Electronic Signature (e-Signature)

Definition (as per IT Act, 2000, Section 2(ta)): "Electronic signature means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature."

This definition highlights that "Electronic Signature" is a broader, umbrella term. It refers to any electronic method used to indicate a person's acceptance, approval, or intent to sign an electronic document.

Characteristics of Electronic Signatures:

- **Intent to Sign:** The core requirement is that the electronic action is performed with the *intent* to sign the document.
- **Variety of Forms:** An e-signature can take various forms, including:
    - Typing your name at the end of an email.
    - Clicking an "I Accept" or "I Agree" button on a website (click-wrap agreement).
    - Pasting a scanned image of your handwritten signature onto a document.
    - Drawing your signature with a mouse or stylus on a touchscreen.
    - Verifying identity through an OTP (One-Time Password) on a mobile number or email.
    - **Aadhaar-based eSign:** This is a specific type of electronic signature in India where the user's identity is authenticated using their Aadhaar number through an e-KYC service, and an OTP/biometric verification confirms their consent to sign the document. This is provided by licensed Certifying Authorities (CAs) and offers a good level of security and legal validity.
- **Legal Recognition (Section 10A):** The IT Act, specifically Section 10A, ensures that a contract formed through electronic means is not invalid or unenforceable *solely* because an electronic form or means was used for its formation.
- **Reliability Criteria (Section 3A):** For an electronic signature to be considered "reliable" (and thus more robust in a legal sense), the IT Act specifies that it must meet certain criteria:
    - The signature creation data (the information used to create the signature) must be uniquely linked to the signatory.
    - The signatory must have sole control over the signature creation data at the time of signing.
    - Any alteration to the electronic signature made after affixing it must be detectable.
    - Any alteration to the information (the document) made after its authentication must be detectable.

Uses of Electronic Signatures: Commonly used for less sensitive documents, internal approvals, HR documents, simple agreements, online forms, and consumer agreements where the risk of repudiation is lower or other contextual evidence supports the transaction.

2. Digital Signature

Definition (as per IT Act, 2000, Section 2(p)): "Digital Signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3."

Key Characteristics of Digital Signatures:

- **Cryptographic Basis:** A digital signature is a *type* of electronic signature that uses advanced cryptographic techniques, specifically **asymmetric cryptography** (Public Key Infrastructure or PKI) and **hash functions**.
- **Public Key Infrastructure (PKI):** This involves a pair of mathematically linked keys:
    - **Private Key:** Known only to the signer, used to create the digital signature.
    - **Public Key:** Widely available, used by others to verify the digital signature.
- **Digital Signature Certificate (DSC):** To use a digital signature, an individual or organization needs a Digital Signature Certificate (DSC). This certificate is issued by a licensed **Certifying Authority (CA)** (regulated by the Controller of Certifying Authorities - CCA in India). The DSC binds the public key to the identity of the individual or organization.
- **Assurance of Identity:** Provides a high level of assurance about the signer's identity because the DSC is issued after due verification by a trusted CA.
- **Ensures Integrity:** The use of a hash function creates a unique "fingerprint" of the document. If even a single character in the document is changed after signing, the digital signature will invalidate, indicating tampering.
- **Non-Repudiation:** Once a document is digitally signed, the signer cannot legitimately deny having signed it, as the private key used to create the signature is unique to them.
- **Audit Trail:** Digital signatures typically embed a timestamp and an audit trail, providing proof of when the document was signed and any actions taken.
- **Higher Security:** Considered more secure and robust than other forms of electronic signatures due to their cryptographic foundation and reliance on trusted third-party CAs.

Uses of Digital Signatures in India: Mandatory or preferred for sensitive transactions, legal documents, and regulatory filings:

- Company filings with the Ministry of Corporate Affairs (MCA)
- Income Tax Return (ITR) e-filing for certain categories of taxpayers
- GST filings
- E-tendering and government procurement
- Signing legal contracts, financial statements, and high-value agreements.

Digital Signature under the IT Act, 2000:

Digital Signatures are a cornerstone of electronic transactions and legal validation in India, primarily governed by the **Information Technology Act, 2000 (IT Act)**, along with its subsequent amendments and related rules. The IT Act provides the legal framework that grants digital signatures the same legal validity as handwritten signatures, thereby facilitating secure and authentic online interactions.

Here's a detailed overview of Digital Signatures under the IT Act, 2000:

1. Legal Recognition (Section 5)

Section 5 of the IT Act is paramount. It explicitly states that where any law requires information to be authenticated by a signature, that requirement is deemed to be satisfied if the information is authenticated by means of a **digital signature** affixed in such manner as may be prescribed by the Central Government. This provision is crucial as it elevates digital signatures to the legal equivalent of physical signatures.

2. Definition of Digital Signature (Section 2(p))

Section 2(p) of the IT Act defines "digital signature" as: "authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3."

3. Authentication of Electronic Records (Section 3)

Section 3 of the IT Act lays down the technical and procedural requirements for authenticating electronic records using a digital signature. It specifies:

- **Asymmetric Crypto System and Hash Function:** The authentication of an electronic record by a digital signature *must* be effected by the use of an asymmetric crypto system and a hash function.
    - **Asymmetric Crypto System (PKI - Public Key Infrastructure):** This involves a pair of cryptographically linked keys: a **private key** (known only to the subscriber/signer) and a **public key** (publicly available). The private key is used by the signer to create the digital signature, and the corresponding public key is used by anyone to verify it.
    - **Hash Function:** This is a mathematical algorithm that generates a unique, fixed-size "hash result" (or "message digest") from an electronic record. Even a minor change in the original electronic record will result in a completely different hash result.
- **Process:**
    1. The electronic record is first put through a **hash function** to create a unique hash result. This hash result digitally "freezes" the document, ensuring its integrity.
    2. This hash result is then encrypted using the signer's **private key**. This encrypted hash is the digital signature.
    3. Any person who has the signer's corresponding **public key** can decrypt the digital signature to retrieve the hash result. They can then independently run the original electronic record through the same hash function.

4. If the hash result obtained from decrypting the signature matches the hash result calculated from the original document, it confirms two things:
    - **Authenticity:** The signature indeed belongs to the person who claims to have signed it (as only their private key could have created that specific encrypted hash).
    - **Integrity:** The electronic record has not been tampered with or altered since it was digitally signed. Any alteration would result in a mismatch of hash values.

- **Non-Repudiation:** Because the private key is uniquely linked to the subscriber and they have sole control over it, they cannot deny having signed the electronic record (unless they can prove the private key was compromised).

4. Digital Signature Certificate (DSC) (Section 2(q) & Chapter VII)

For a digital signature to be legally valid and verifiable, it must be accompanied by a **Digital Signature Certificate (DSC)**.

- **Section 2(q):** Defines "Digital Signature Certificate" as a Digital Signature Certificate issued under sub-section (4) of section 35.
- **Chapter VII (Sections 35-39):** Deals with the issuance, suspension, and revocation of DSCs. A DSC is essentially an electronic credential that binds the public key to the identity of the individual or organization to whom it has been issued.
- **Contents of DSC (Section 35(4)):** A DSC typically contains:
    - The public key of the subscriber.
    - The name of the subscriber.
    - The identity of the Certifying Authority (CA) that issued the certificate.
    - The validity period of the the certificate.
    - The digital signature of the CA (which certifies the authenticity of the DSC itself).

5. Certifying Authorities (CAs) and Controller of Certifying Authorities (CCA) (Chapter VI)

The IT Act establishes a robust regulatory framework for digital signatures:

- **Controller of Certifying Authorities (CCA) (Section 17):** The Central Government appoints a CCA who acts as the root authority for digital signatures in India. The CCA licenses and supervises the Certifying Authorities.
- **Certifying Authorities (CAs):** These are trusted third-party entities licensed by the CCA to issue, suspend, and revoke Digital Signature Certificates. CAs play a crucial role in verifying the identity of the applicant before issuing a DSC, thereby ensuring the trustworthiness of the entire system. Examples of licensed CAs in India include eMudhra, Sify, NSDL, Capricorn, etc.

- **Duties of CAs (Section 30):** The IT Act outlines the duties of CAs, including ensuring the security of their systems, adhering to prescribed standards, and maintaining records.

6. Secure Digital Signature (Section 15)

Section 15 defines when a digital signature is considered "secure." A digital signature is deemed secure if:

- The **signature creation data** (i.e., the private key) was, at the time of affixing the signature, under the exclusive control of the signatory and no other person.
- The signature creation data was stored and affixed in such an exclusive manner as may be prescribed (typically on a hardware cryptographic token like a USB dongle).

7. Evidentiary Value (Indian Evidence Act, 1872 amendments)

The IT Act, 2000 also brought necessary amendments to the **Indian Evidence Act, 1872**, to ensure the admissibility and evidentiary value of electronic records and digital signatures in court:

- **Section 3 (Definition of Evidence):** Expanded to include electronic records as "documents."
- **Section 65B (Admissibility of Electronic Records):** Lays down the conditions for the admissibility of electronic records as evidence.
- **Section 67A (Proof as to electronic signature):** Provides for the presumption of authenticity of a secure electronic signature.
- **Section 85B (Presumption as to electronic records and digital signatures):** States that a secure electronic record shall be presumed to have not been altered, and a secure digital signature shall be presumed to be affixed with the intention of signing or approving the electronic record.

Documents Exempt from Digital Signature

It's important to note that while digital signatures are widely applicable, the First Schedule of the IT Act, 2000, specifies certain documents that *cannot* be executed through electronic means (including digital signatures) and still require a physical, "wet" signature for legal validity. These include:

- Negotiable Instruments (other than cheques)
- Powers of Attorney
- Trusts
- Wills and any other testamentary disposition
- Any contract for the sale or conveyance of immovable property or any interest in such property.

E- Governance Attribution, Acknowledgement and Dispatch of Electronic Records:

E-Governance, or electronic governance, signifies the application of Information and Communication Technologies (ICTs) by the government to enhance efficiency, effectiveness, transparency, and accountability in the delivery of government services, exchange of information, communication

transactions, and integration of various standalone systems. It essentially digitalizes government functions and interactions with citizens, businesses, and other government entities.

The **Information Technology Act, 2000 (IT Act)** plays a pivotal role in enabling e-governance in India by providing the legal framework for electronic records and transactions. Chapter IV of the IT Act, specifically Sections 11, 12, and 13, are crucial for establishing the legal certainty around the **attribution, acknowledgement, and dispatch of electronic records**, which are fundamental to the operation of e-governance systems.

I. E-Governance under the IT Act, 2000

The IT Act provides legal backing for e-governance through several key provisions:

- **Section 4 (Legal Recognition of Electronic Records):** Ensures that information in electronic form is legally valid, giving legal sanctity to government documents, applications, and communications exchanged digitally.
- **Section 5 (Legal Recognition of Electronic Signatures):** Grants legal equivalence to electronic signatures (including digital signatures) with handwritten signatures. This is vital for authenticating government documents, citizen applications, and approvals in the digital realm.
- **Section 6 (Use of Electronic Records and Digital Signatures in Government and its Agencies):** This is a direct enabler for e-governance. It states that where any law provides for:
    - The filing of any form, application, or other document with any office, authority, or body.
    - The issue or grant of any license, permit, sanction, or approval by whatever name called.
    - The receipt or payment of money in a particular manner.
    - Such requirement shall not be deemed to have been satisfied unless such filing, issue, grant, receipt, or payment, as the case may be, is effected by means of **electronic form** as may be prescribed by the appropriate Government. This section empowers governments to mandate electronic transactions.
- **Section 6A (Service of documents by electronic means):** Allows for the service of documents (e.g., summons, notices, orders) by electronic means, provided rules are made by the appropriate government.
- **Section 7 (Retention of Electronic Records):** Provides for the legal validity of electronic records retained as required by law.
- **Section 8 (Publication of Rules, Regulations, etc., in Electronic Gazette):** Facilitates the official publication of rules, regulations, orders, and other legal instruments in an electronic format (the Electronic Gazette), giving them legal validity.

II. Attribution of Electronic Records (Section 11)

In the digital world, it can be challenging to definitively link an electronic record to its sender. Section 11 of the IT Act addresses this by providing clear rules for the **attribution** of electronic records to the **originator**. An electronic record is attributed to the originator if it was sent by:

1. **The originator himself:** This is the direct act of sending by the person who created or intended to send the record.
2. **A person who had the authority to act on behalf of the originator:** This covers situations where an agent or authorized representative sends the record on behalf of the originator (e.g., an assistant sending an email on a manager's behalf).
3. **An information system programmed by or on behalf of the originator to operate automatically:** This is critical for automated government services. For example, if a government portal automatically generates and sends an acknowledgment or a certificate based on predefined rules after an application is submitted, that electronic record is attributed to the government agency (the originator).

Importance for E-Governance: This section is vital for establishing accountability and legal validity in automated government processes. It clarifies that electronic records generated by government systems are indeed from the government, even without a human directly pressing "send."

III. Acknowledgement of Receipt of Electronic Records (Section 12)

In traditional communication, confirmation of receipt is often manual. Section 12 deals with the **acknowledgement of receipt** of electronic records, which is crucial for contracts and official communications in e-governance.

1. **No Stipulation by Originator:** If the originator has not specified a particular form or method for acknowledgment, then acknowledgment may be given by:
    - Any communication by the addressee (automated or otherwise), e.g., a reply email, an automated "read receipt."
    - Any conduct of the addressee sufficient to indicate to the originator that the electronic record has been received (e.g., taking action based on the received information).
2. **Stipulation by Originator (Binding on Receipt):** If the originator has explicitly stated that the electronic record shall be binding *only upon receipt of an acknowledgment*, then:
    - Unless such acknowledgment is received, the electronic record is deemed to have *never been sent* by the originator. This protects the originator from being bound by an unreceived communication.
3. **No Stipulation by Originator (No Acknowledgment Received):** If the originator has *not* stipulated that the record is binding only on acknowledgment, but no acknowledgment is received within the specified time (or a reasonable time if no time is specified), the originator may:
    - Give notice to the addressee that no acknowledgment has been received and specify a reasonable time by which the acknowledgment must be received.
    - If no acknowledgment is received within that extended time, the originator may, after giving notice to the addressee, treat the electronic record as though it has never been sent.

Importance for E-Governance: This ensures certainty in digital communication flows between government and citizens/businesses. For instance, when a citizen applies for a service online, the

government portal often provides an immediate automated acknowledgment. Section 12 clarifies the legal implications of such acknowledgments.

IV. Dispatch of Electronic Records (Section 13)

Section 13 determines the **time and place of dispatch and receipt** of electronic records. This is critical for establishing when a legal obligation begins or ends, especially in contractual or time-sensitive government processes.

1. **Time of Dispatch:**
    - Unless otherwise agreed, the dispatch of an electronic record occurs when it **enters a computer resource outside the control of the originator.**
    - *Example:* When you click "send" on an email, and it leaves your outbox and enters your email provider's server (which is outside your direct control), that is the time of dispatch.
2. **Time of Receipt:**
    - **If the addressee has designated a computer resource (e.g., a specific email address, a specific server) for receiving electronic records:**
        - Receipt occurs when the electronic record **enters that designated computer resource.**
        - If the electronic record is sent to a computer resource *not* designated by the addressee, receipt occurs when the electronic record is **retrieved by the addressee.**
    - **If the addressee has NOT designated a computer resource:**
        - Receipt occurs when the electronic record **enters the computer resource of the addressee.**
3. **Place of Dispatch and Receipt:**
    - Unless otherwise agreed, an electronic record is deemed to be **dispatched at the place where the originator has their place of business.**
    - It is deemed to be **received at the place where the addressee has their place of business.**
    - If there are multiple places of business, the **principal place of business** is considered.
    - If no place of business, the **usual place of residence** is considered (for a body corporate, this means its registered place).

Importance for E-Governance: This section provides clarity on jurisdiction and timelines for legal purposes in e-governance. For example, it determines when a digitally filed application is legally considered submitted or when an e-notice is legally considered served.

In summary, Chapter IV of the IT Act, 2000, provides essential legal clarity for the fundamental aspects of electronic communication in e-governance – ensuring that digital records can be reliably linked to their source, that their receipt can be confirmed, and that the time and place of their dispatch and receipt are legally defined, thereby fostering trust and accountability in India's digital public services.

Certifying Authorities:

In the context of the **Information Technology Act, 2000 (IT Act)** of India, **Certifying Authorities (CAs)** are the foundational pillars of trust and authenticity in the digital signature ecosystem. They are the entities responsible for issuing, managing, and revoking Digital Signature Certificates (DSCs), which are crucial for validating digital signatures.

Role of Certifying Authorities

A Certifying Authority (CA) acts as a trusted third party in the Public Key Infrastructure (PKI). Their primary role is to verify the identity of individuals or organizations and then issue them a Digital Signature Certificate (DSC) that binds their public key to their verified identity. This process is analogous to a government body issuing a passport or a driver's license, where the issuing authority verifies your identity before granting you an official document.

Legal Basis under the IT Act, 2000

The IT Act, 2000, dedicates an entire chapter (Chapter VI, Sections 17 to 34) to the regulation of Certifying Authorities.

1. **Controller of Certifying Authorities (CCA) - The Regulator (Section 17):**
    - The Central Government appoints a **Controller of Certifying Authorities (CCA)**.
    - The CCA is the primary regulatory body responsible for overseeing the activities of CAs in India.
    - **Functions of the CCA (Section 18):**
        - Licensing and regulating the working of Certifying Authorities.
        - Laying down the standards that CAs must maintain.
        - Specifying the qualifications and experience required for employees of CAs.
        - Specifying the conditions under which CAs shall conduct their business.
        - Auditing the CAs to ensure compliance.
        - Certifying the public keys of the CAs themselves (through the Root Certifying Authority of India - RCAI), which is essential for the entire trust hierarchy.
        - Maintaining a National Repository of Digital Certificates (NRDC) containing all certificates issued by CAs.
        - Investigating contraventions of the Act.
2. **License to Issue DSCs (Section 21):**
    - Any person who wishes to operate as a Certifying Authority must apply to the CCA for a license.
    - The CCA grants the license based on the applicant meeting prescribed criteria, including financial standing, technical infrastructure, and security procedures.
3. **Conditions for Grant of License (Section 22):**
    - The CCA considers various factors, including the financial and human resources, the security systems, and the proposed certification practice statement of the applicant.

- The applicant must furnish a security guarantee (e.g., bank guarantee) to ensure compliance with the Act and rules.

Powers and Functions of Certifying Authorities (CAs)

Once licensed, a Certifying Authority performs several crucial functions:

1. **Issuance of Digital Signature Certificates (DSCs):**
   - This is the primary function. CAs verify the identity of the applicant (individual, organization, device) through various means, including Aadhaar e-KYC, physical verification, video verification, and document submission.
   - Upon successful verification, they issue a DSC, which contains the subscriber's public key, identity details, and the CA's own digital signature.
2. **Revocation and Suspension of DSCs (Section 38):**
   - CAs have the authority to suspend or revoke a DSC if:
     - The subscriber requests it.
     - The subscriber dies or is declared legally incompetent.
     - There is a material misrepresentation or fraud in obtaining the certificate.
     - The private key associated with the DSC is compromised.
     - The certificate was issued without proper authorization.
   - This ensures the integrity and trustworthiness of the digital signature system.
3. **Publication of Information (Section 34):**
   - CAs are required to make certain disclosures, including:
     - Their own Digital Signature Certificate.
     - Their **Certification Practice Statement (CPS)**, which details the practices, policies, and procedures they employ in issuing and managing DSCs.
     - Notice of revocation or suspension of any DSCs they have issued.
     - Any facts that materially and adversely affect the reliability of a DSC.
4. **Adherence to Security Procedures (Section 30):**
   - CAs must implement robust hardware, software, and procedures that are secure from intrusion and misuse.
   - They must provide a reasonable level of reliability in their services and adhere to security procedures to ensure the secrecy and privacy of electronic signatures.
   - They must ensure their systems comply with specified standards and audit requirements.
5. **Maintenance of Records:**
   - CAs are required to maintain records related to the issuance, suspension, and revocation of DSCs for a specified period.
6. **Compliance with the Act and Rules (Section 31):**
   - CAs must ensure that all their employees and anyone engaged by them comply with the provisions of the IT Act, rules, regulations, and orders made thereunder.
7. **Display of License (Section 32):**
   - Every Certifying Authority must prominently display its license at its place of business.

Types of Digital Signature Certificates Issued by CAs in India

CAs in India issue different classes of DSCs, based on the level of identity verification and security requirements:

- **Class 1 DSC (No longer issued/relevant for most official purposes):** Provided a basic level of assurance and was used for low-risk environments where the user's name and email were verified against a database.
- **Class 2 DSC (Largely phased out or subsumed by Class 3 for most new uses):** Used to confirm the identity of the signer against a pre-verified database. Commonly used for e-filing of Income Tax Returns, Goods and Services Tax (GST) returns, MCA filings (for company and LLP registration/compliance), etc.
- **Class 3 DSC (Highest Security Level, most common now):** Requires the applicant to physically present themselves before a Registration Authority (RA) or undergo stringent video verification for identity authentication. It offers the highest level of security and is mandatory for high-value transactions, e-tendering, e-procurement, e-auctions, court filings, and other critical government and corporate applications.
- **DGFT DSC:** A specific type of DSC used for obtaining Import Export Code (IEC) and for foreign trade-related transactions.
- **Sign, Encrypt, and Combo DSCs:** CAs often offer different types based on functionality:
    - **Signing DSC:** Used solely for signing documents (e.g., PDF, XML).
    - **Encryption DSC:** Used to encrypt documents, ensuring confidentiality. Only the intended recipient with the corresponding private key can decrypt it.
    - **Combo DSC:** Combines both signing and encryption capabilities in a single certificate.

List of Licensed Certifying Authorities in India

Some of the prominent licensed Certifying Authorities operating in India include:

- eMudhra Limited
- Capricorn Identity Services Private Limited
- XtraTrust DigiSign Private Limited
- PantaSign Securities Private Limited
- Safescrypt CA Services (Sify Communications Ltd.)
- National Informatics Centre (NIC)
- IDRBT Certifying Authority
- (n)Code Solutions CA (Gujarat Narmada Valley Fertilizers & Chemicals Ltd.)
- Verasys Technologies Private Limited

The Certifying Authorities, under the strict supervision of the Controller of Certifying Authorities, form the backbone of trust and security for digital interactions in India, making e-governance and e-commerce legally viable and dependable.

Electronic Signature Certificates:

In India, the term "Electronic Signature Certificate" can be a bit confusing because the **Information Technology Act, 2000 (IT Act)**, as amended, primarily focuses on **Digital Signature Certificates (DSCs)** and, more recently, on the broader concept of **eSign** (Aadhaar-based electronic signature service).

Let's clarify what "Electronic Signature Certificate" refers to under Indian law, especially in relation to Digital Signature Certificates.

Electronic Signature Certificate (ESC) - The Broader Term

Section 2(tb) of the IT Act, 2000, defines "Electronic Signature Certificate" as: "an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate."

This definition makes it clear that **Digital Signature Certificates (DSCs) are a *type* of Electronic Signature Certificate.** The broader term "Electronic Signature Certificate" encompasses any certificate issued to authenticate an electronic signature, irrespective of the underlying technology, as long as it meets the reliability criteria prescribed by the Central Government.

However, in common parlance and in practice, when people refer to "certificates" for electronic signing, they are almost exclusively talking about **Digital Signature Certificates (DSCs)**. The prominent example of another *type* of electronic signature that technically falls under the broader ESC umbrella, and has its own associated "certificate-like" process (though not a physical file certificate in the same way as a DSC), is the **Aadhaar-based eSign service.**

Digital Signature Certificate (DSC) - The Specific Implementation

As discussed previously, a Digital Signature Certificate (DSC) is the most common and robust form of Electronic Signature Certificate in India.

Key aspects of a DSC:

- **Cryptographic Basis:** It's based on Public Key Infrastructure (PKI), using asymmetric cryptography.
- **Issued by CAs:** Issued by licensed Certifying Authorities (CAs) under the strict regulation of the Controller of Certifying Authorities (CCA).
- **Verifies Identity:** Binds a public key to the identity of the subscriber (individual, organization, device) after rigorous verification by the CA.
- **Ensures Integrity:** Through hash functions, it guarantees that the signed document has not been tampered with since it was signed.
- **Non-Repudiation:** Provides strong legal evidence that the signer cannot deny having signed the document.

- **Validity:** Has a specific validity period (typically 1, 2, or 3 years) and can be suspended or revoked by the CA under certain conditions.
- **Physical Form (typically):** Often stored on a secure hardware cryptographic token (like a USB dongle) to ensure the private key remains under the sole control of the signer.

Aadhaar-based eSign - A Newer Form of Electronic Signature

While not typically issued as a separate "certificate file" in the same way as a DSC, the **Aadhaar-based eSign service** is an important "electronic authentication technique" (as per the Second Schedule of the IT Act, read with Section 3A). The process involves a temporary, transaction-specific certificate generation.

How Aadhaar-based eSign works:

1. **Authentication:** The signer provides their Aadhaar number or Virtual ID (VID) to an eSign Service Provider (ESP).
2. **OTP/Biometric Verification:** Authentication is done via an OTP sent to the mobile number linked with Aadhaar or through biometric authentication (fingerprint/iris scan).
3. **Digital Signature Generation:** Upon successful authentication, a secure digital signature is generated on a Hardware Security Module (HSM) by the ESP (which is typically a licensed CA). This digital signature is affixed to the document.
4. **Temporary Certificate:** A temporary, one-time-use Digital Signature Certificate (DSC) is generated and used for that specific signing instance, often destroyed immediately after use.
5. **Legality:** Aadhaar-based eSign is legally recognized under the IT Act and is widely accepted for various transactions due to its ease of use and strong authentication method.

Duties of Subscribers:

In India, the **Information Technology Act, 2000 (IT Act)**, particularly **Chapter VIII (Sections 40 to 42)**, outlines the crucial **duties of subscribers** of Digital Signature Certificates (DSCs) and Electronic Signature Certificates (ESCs). These duties are essential to maintain the integrity, security, and legal validity of electronic transactions authenticated by these signatures.

A "subscriber" is defined in **Section 2(1)(zg)** of the IT Act as "a person in whose name the Electronic Signature Certificate is issued."

Here are the key duties of subscribers:

1. Generating Key Pair (Section 40)

Where a Digital Signature Certificate (DSC) has been accepted by a subscriber, it is the subscriber's duty to **generate the key pair** (consisting of the public key and the corresponding private key) by applying the prescribed **security procedure**.

- **Public Key:** This is the key listed in the Digital Signature Certificate and is made public for verifying the signature.
- **Private Key:** This is the secret key that must remain under the sole control of the subscriber, used for creating the digital signature.
- **Security Procedure (as per Section 16):** This refers to the security measures, processes, and precautions that must be observed to ensure the secure creation and handling of the keys, preventing their disclosure or compromise. This typically involves the use of a secure hardware device like a USB crypto token to store the private key.

2. Duties of Subscriber of Electronic Signature Certificate (Section 40A)

This section, inserted by the IT (Amendment) Act, 2008, broadened the scope to include all electronic signatures. It states that in respect of an Electronic Signature Certificate, the subscriber shall perform **such duties as may be prescribed**. This gives the Central Government the power to specify duties for other types of electronic signatures (like Aadhaar-based eSign) through rules and regulations.

3. Acceptance of Digital Signature Certificate (Section 41)

A subscriber is deemed to have **accepted a Digital Signature Certificate** if they:

- **Publish or authorize the publication** of the DSC to one or more persons or in a repository (e.g., the National Repository of Digital Certificates).
- **Otherwise demonstrate their approval** of the DSC in any manner.

By accepting a DSC, the subscriber implicitly **certifies** to anyone who reasonably relies on the information contained in that DSC that:

- **They hold and are entitled to hold the private key** corresponding to the public key listed in the DSC. This means they are the legitimate user of the certificate.
- **All representations made by the subscriber to the Certifying Authority (CA) and all material information contained in the DSC are true.** This places a responsibility on the subscriber to provide accurate information during the DSC application process.
- **All information contained in the DSC that is within the knowledge of the subscriber is true.** This emphasizes the subscriber's ongoing responsibility for the accuracy of information known to them.

4. Control of Private Key (Section 42)

This is one of the most critical duties for ensuring the security and validity of digital signatures.

- **Duty of Reasonable Care:** Every subscriber must exercise **reasonable care** to retain control of the private key corresponding to the public key listed in their Digital Signature Certificate. They must also take **all necessary steps to prevent its disclosure** to unauthorized persons.

- **Duty to Communicate Compromise:** If the private key corresponding to the public key listed in the DSC has been **compromised** (e.g., lost, stolen, or suspected of being copied), the subscriber **must communicate the same without any delay to the Certifying Authority (CA)** in the manner specified by regulations.
- **Liability until Communication:** For the removal of doubts, the Act explicitly states that the **subscriber shall be liable until they have informed the Certifying Authority that the private key has been compromised.** This provision is vital as it clarifies the subscriber's legal responsibility for any transactions signed using the compromised key until the CA is notified and can take action (e.g., suspend the DSC).

Implications of Duties

Fulfilling these duties is not merely a procedural requirement but carries significant legal implications:

- **Legal Validity:** Adherence to these duties ensures that the digital signature carries its full legal weight and evidentiary value.
- **Prevention of Misuse:** Proper control of the private key and prompt reporting of compromise are essential to prevent fraudulent use of the DSC.
- **Liability:** Failure to comply with these duties, especially regarding the control and reporting of a compromised private key, can result in the subscriber being held liable for unauthorized transactions or legal consequences arising from the misuse of their digital signature.
- **Certificate Revocation:** Non-compliance or a breach of these duties (e.g., misrepresentation of facts) can lead to the suspension or revocation of the Digital Signature Certificate by the Certifying Authority.

In essence, while Certifying Authorities provide the trusted infrastructure for digital signatures, the ultimate responsibility for the secure and proper use of a DSC largely rests with the subscriber, making them a crucial link in the chain of digital trust.

Penalties and Offences:

In India, penalties and offenses related to cybercrime are primarily governed by the **Information Technology Act, 2000 (IT Act)**, as amended by the IT (Amendment) Act, 2008. Additionally, certain cybercrimes also fall under the purview of the **Indian Penal Code, 1860 (IPC)**, especially when they involve traditional offenses committed through digital means.

It's important to note that the IT Act focuses specifically on offenses related to computers, computer systems, and networks, while the IPC covers a broader range of criminal acts, some of which can be facilitated by technology.

I. Penalties and Offences under the Information Technology Act, 2000

The IT Act defines various cyber offenses and prescribes corresponding penalties. Here's a summary of some of the most significant sections:

A. Offences related to Data & Systems (often with compensation/penalty to the affected party):

- **Section 43: Penalty and Compensation for Damage to Computer, Computer System, etc.**
  - **Offense:** Unauthorized access, downloading, extracting, introducing viruses, disrupting computer systems, denying access to authorized persons, charging for services not availed, tampering with computer networks, destroying information, or disrupting services.
  - **Penalty:** The person who causes such damage or loss is liable to pay **damages by way of compensation** to the affected person. The amount of compensation can be substantial, sometimes extending to ₹5 crore or more, depending on the loss caused. This is a civil wrong.
- **Section 43A: Compensation for Failure to Protect Data**
  - **Offense:** If a body corporate possessing, dealing, or handling sensitive personal data or information in a computer resource is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person.
  - **Penalty:** The body corporate shall be liable to pay **damages by way of compensation** to the person so affected.
- **Section 44: Penalty for Failure to Furnish Information, Return, etc.**
  - **Offense:** Failure to furnish documents, returns, or reports, or to maintain books of accounts or records as required by the Act or rules.
  - **Penalty:** Monetary penalties, e.g., up to ₹1.5 lakh for not furnishing documents, or ₹5,000 per day for continuing default.
- **Section 45: Residuary Penalty**
  - **Offense:** Any contravention of the Act or its rules for which no specific penalty has been provided elsewhere.
  - **Penalty:** May extend to ₹25,000 and, in case of continuing contravention, an additional penalty of up to ₹5,000 for every day after the first contravention.

B. Criminal Offences (with Imprisonment and/or Fines):

- **Section 65: Tampering with Computer Source Documents**
  - **Offense:** Intentionally concealing, destroying, or altering any computer source code (which is required to be kept or maintained).
  - **Penalty:** Imprisonment up to 3 years, or fine up to ₹2,00,000, or both.
- **Section 66: Computer Related Offences (Hacking, Data Theft, etc.)**
  - **Offense:** Any person who commits an act specified in Section 43 (unauthorized access, data theft, causing damage, etc.) with dishonest or fraudulent intention. This converts the civil wrong under Section 43 into a criminal offense.
  - **Penalty:** Imprisonment up to 3 years, or fine up to ₹5,00,000, or both.

- **Section 66B: Punishment for Dishonestly Receiving Stolen Computer Resource or Communication Device**
  - **Offense:** Receiving or retaining any stolen computer, computer system, or communication device, knowing or having reason to believe it is stolen.
  - **Penalty:** Imprisonment up to 3 years, or fine up to ₹1,00,000, or both.
- **Section 66C: Punishment for Identity Theft**
  - **Offense:** Fraudulently or dishonestly making use of the electronic signature, password, or any other unique identification feature of another person.
  - **Penalty:** Imprisonment up to 3 years, or fine up to ₹1,00,000, or both.
- **Section 66D: Punishment for Cheating by Personation by Using Computer Resource**
  - **Offense:** Cheating by pretending to be another person using a computer resource or any communication device. (Often used for online fraud, phishing, job scams).
  - **Penalty:** Imprisonment up to 3 years, or fine up to ₹1,00,000, or both.
- **Section 66E: Punishment for Violation of Privacy (Publishing Private Images)**
  - **Offense:** Capturing, publishing, or transmitting the image of a private area of any person without their consent, in circumstances violating their privacy. (Commonly known as "Revenge Pornography").
  - **Penalty:** Imprisonment up to 3 years, or fine up to ₹2,00,000, or both.
- **Section 66F: Punishment for Cyber Terrorism**
  - **Offense:** Committing or conspiring to commit acts with intent to threaten the unity, integrity, security, or sovereignty of India, or to strike terror in people, by:
    - Denying access to a computer resource.
    - Unauthorized access to a computer resource.
    - Introducing contaminants, viruses, or other harmful computer code.
    - Disrupting critical information infrastructure.
  - **Penalty:** Imprisonment which may extend to **imprisonment for life**. (This is a very serious offense).
- **Section 67: Punishment for Publishing or Transmitting Obscene Material in Electronic Form**
  - **Offense:** Publishing or transmitting any material that is lascivious or appeals to the prurient interest, or if its effect is to tend to deprave and corrupt persons.
  - **Penalty:**
    - First conviction: Imprisonment up to 3 years and fine up to ₹5,00,000.
    - Subsequent conviction: Imprisonment up to 5 years and fine up to ₹10,00,000.
- **Section 67A: Punishment for Publishing or Transmitting Material Containing Sexually Explicit Act, etc., in Electronic Form**
  - **Offense:** Publishing or transmitting any material that contains sexually explicit acts or conduct.
  - **Penalty:**
    - First conviction: Imprisonment up to 5 years and fine up to ₹10,00,000.
    - Subsequent conviction: Imprisonment up to 7 years and fine up to ₹10,00,000.
- **Section 67B: Punishment for Publishing or Transmitting Material Depicting Children in Sexually Explicit Act, etc., in Electronic Form (Child Pornography)**

- **Offense:** Publishing or transmitting any material that depicts children in sexually explicit acts or conduct.
- **Penalty:**
  - First conviction: Imprisonment up to 5 years and fine up to ₹10,00,000.
  - Subsequent conviction: Imprisonment up to 7 years and fine up to ₹10,00,000.
- **Note:** This section often overlaps with the stricter provisions of the Protection of Children from Sexual Offences (POCSO) Act, 2012, which carries even higher penalties for child sexual abuse material.

- **Section 68: Power of Controller to Give Directions**
  - **Offense:** Failure or refusal to comply with any direction given by the Controller of Certifying Authorities (CCA).
  - **Penalty:** Imprisonment up to 2 years, or fine up to ₹1,00,000, or both.
- **Section 69: Power to Issue Directions for Interception or Monitoring or Decryption of Any Information**
  - **Offense:** Failure by any intermediary to assist the agency authorized to intercept, monitor, or decrypt information.
  - **Penalty:** Imprisonment up to 7 years and fine.
- **Section 69A: Power to Issue Directions for Blocking for Public Access of Any Information**
  - **Offense:** Failure by any intermediary to comply with Government directions to block public access to certain information.
  - **Penalty:** Imprisonment up to 7 years and fine.
- **Section 70: Protected System**
  - **Offense:** Securing or attempting to secure unauthorized access to a "protected system" (critical information infrastructure as declared by the government).
  - **Penalty:** Imprisonment up to 10 years, and fine.
- **Section 71: Penalty for Misrepresentation**
  - **Offense:** Making any misrepresentation or suppressing any material fact to the Controller or a Certifying Authority for obtaining any license or Digital Signature Certificate.
  - **Penalty:** Imprisonment up to 2 years, or fine up to ₹1,00,000, or both.
- **Section 72: Penalty for Breach of Confidentiality and Privacy**
  - **Offense:** Any person who has secured access to any electronic record, book, register, correspondence, information, document, or other material, without the consent of the person concerned, discloses such information to any other person.
  - **Penalty:** Imprisonment up to 2 years, or fine up to ₹1,00,000, or both.
- **Section 72A: Punishment for Disclosure of Information in Breach of Lawful Contract**
  - **Offense:** Providing services under the terms of a lawful contract, and with the intent to cause wrongful loss or wrongful gain, discloses personal information of another person without their consent or in breach of a lawful contract.
  - **Penalty:** Imprisonment up to 3 years, or fine up to ₹5,00,000, or both.
- **Section 73: Penalty for Publishing Electronic Signature Certificate False in Certain Particulars**

- **Offense:** Publishing or making available an ESC with knowledge that the CA listed did not issue it, or that the subscriber listed has not accepted it, or that it has been revoked or suspended (without indicating so).
- **Penalty:** Imprisonment up to 2 years, or fine up to ₹1,00,000, or both.

- **Section 74: Publication for Fraudulent Purpose**
  - **Offense:** Knowingly creating, publishing, or otherwise making available an ESC for any fraudulent or unlawful purpose.
  - **Penalty:** Imprisonment up to 2 years, or fine up to ₹1,00,000, or both.

II. Penalties and Offences under the Indian Penal Code, 1860 (IPC) for Cybercrimes

Many traditional offenses, when committed with the aid of computers or the internet, are also punishable under the IPC. The IT Act often supplements or is used in conjunction with the IPC for comprehensive prosecution.

- **Section 354D: Stalking**
  - **Offense:** Includes following a person, contacting them, or monitoring their electronic communication (e.g., email, internet, social media) despite a clear indication of disinterest.
  - **Penalty:** First conviction: Imprisonment up to 3 years and fine. Subsequent conviction: Imprisonment up to 5 years and fine.
- **Section 379: Theft**
  - **Offense:** Dishonestly taking any movable property out of the possession of any person without that person's consent. (Can apply to theft of digital devices like mobile phones, laptops if the intent is to permanently deprive).
  - **Penalty:** Imprisonment up to 3 years, or fine, or both.
- **Section 411: Dishonestly Receiving Stolen Property**
  - **Offense:** Receiving or retaining any movable property, knowing or having reason to believe it to be stolen. (Applicable to stolen digital devices).
  - **Penalty:** Imprisonment up to 3 years, or fine, or both.
- **Section 419: Punishment for Cheating by Personation**
  - **Offense:** Cheating by pretending to be some other person. (Used in conjunction with IT Act Section 66D for online impersonation/fraud).
  - **Penalty:** Imprisonment up to 3 years, or fine, or both.
- **Section 420: Cheating and Dishonestly Inducing Delivery of Property**
  - **Offense:** Cheating and dishonestly inducing the person deceived to deliver any property, or to make, alter, or destroy the whole or any part of a valuable security. (Widely used in online financial frauds, phishing, scams, where money or property is illegally obtained).
  - **Penalty:** Imprisonment up to 7 years and fine.
- **Sections 463 to 471: Forgery**
  - **Offense:** Making false documents or electronic records with intent to cause damage or injury, or to support any claim, or to cause any person to part with property. (Applicable to creating fake websites, emails, or digital documents for fraudulent purposes).

- **Penalty:** Varies depending on the specific section and purpose of forgery, up to 7 years imprisonment.

- **Section 499/500: Defamation**
  - **Offense:** Making or publishing any imputation concerning any person intending to harm, or knowing it is likely to harm, the reputation of that person. (Applicable to online defamation via social media, blogs, etc.).
  - **Penalty:** Imprisonment up to 2 years, or fine, or both.
- **Section 503/506/507: Criminal Intimidation**
  - **Offense:** Threatening another person with injury to their person, reputation, or property, with intent to cause alarm or to compel them to do something they are not legally bound to do. (Applicable to online threats, cyberbullying with threats).
  - **Penalty:** Varies from 2 years to 7 years imprisonment, or fine, or both, depending on the severity and method (e.g., anonymous communication).
- **Section 509: Word, Gesture or Act Intended to Insult the Modesty of a Woman**
  - **Offense:** Uttering any word, making any sound or gesture, or exhibiting any object, intending to insult the modesty of any woman. (Often applied to online sexual harassment, abusive messages).
  - **Penalty:** Simple imprisonment up to 1 year, or fine, or both.
- **Sections 292, 293, 294: Obscenity**
  - **Offense:** Deals with the sale, distribution, or public display of obscene material. (Used in conjunction with IT Act Sections 67, 67A, 67B for online pornography, distribution of obscene content).
  - **Penalty:** Varies, but can include imprisonment and fine.

Intermediaries:

In India, "Intermediaries" play a crucial role in the digital ecosystem, facilitating the flow of information and services online. Their regulation is primarily governed by the **Information Technology Act, 2000 (IT Act)**, particularly **Section 79**, which provides a "safe harbor" or exemption from liability for third-party content under certain conditions, and the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021)**, which lay down specific due diligence obligations.

I. Definition of "Intermediary"

Section 2(1)(w) of the IT Act, 2000, defines an "Intermediary" with respect to any particular electronic records as: "any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes."

This definition is broad and encompasses a wide range of entities that enable or facilitate online activities without necessarily creating the content themselves. Examples include:

- **Internet Service Providers (ISPs)**
- **Telecom Service Providers (TSPs)**
- **Social Media Platforms** (Facebook, X (formerly Twitter), Instagram, YouTube, WhatsApp, etc.)
- **Search Engines** (Google, Bing)
- **Online Marketplaces** (Amazon, Flipkart)
- **Online Payment Gateways** (Paytm, Google Pay)
- **Cloud Service Providers**
- **Web Hosting Companies**
- **App Stores**
- **Online Gaming Platforms** (explicitly covered under IT Rules, 2021)
- **News Aggregators and Digital Media Publishers** (also brought under the IT Rules, 2021)

II. Intermediary Liability and "Safe Harbor" (Section 79)

Section 79 of the IT Act is the cornerstone of intermediary liability in India. It provides a "safe harbor" protection, meaning an intermediary shall **not be liable** for any third-party information, data, or communication link made available or hosted by them, *provided* certain conditions are met.

A. Conditions for Availing Safe Harbor (Section 79(2)):

For an intermediary to claim safe harbor, their function must be limited to a "passive" role, implying they do not have active control over the content. Specifically, the exemption applies if:

1. **Limited Function:** The intermediary's function is limited to providing access to a communication system over which information made available by third parties is transmitted, or temporarily stored, or hosted.
2. **No Initiation, Selection, or Modification:** The intermediary does not:
    - Initiate the transmission.
    - Select the receiver of the transmission.
    - Select or modify the information contained in the transmission.
3. **Due Diligence:** The intermediary observes due diligence while discharging its duties under the Act and also observes such other guidelines as the Central Government may prescribe (these are the IT Rules, 2021).

B. When Safe Harbor Does NOT Apply (Section 79(3)):

The safe harbor protection is lost, and the intermediary can be held liable if:

1. **Active Participation:** The intermediary has conspired, abetted, aided, or induced (whether by threats or promise or otherwise) the commission of the unlawful act. This implies a more active role or complicity.
2. **Failure to Act on Knowledge/Notice:** Upon receiving actual knowledge, or on being notified by the appropriate Government or its agency, that any information residing in or connected to a computer resource controlled by the intermediary is being used to commit an unlawful act, the intermediary fails to expeditiously remove or disable access to that material.
    - The landmark Supreme Court judgment in **Shreya Singhal v. Union of India (2015)** clarified that "actual knowledge" must be derived from a **court order or a notification from the appropriate Government or its agency**, not merely from private complaints. This was a crucial interpretation to prevent self-censorship and over-blocking by intermediaries.

III. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

These rules, superseding the 2011 rules, significantly enhance the due diligence obligations of intermediaries, especially for "Significant Social Media Intermediaries" (SSMIs - those with over 50 lakh registered users in India). They aim to make intermediaries more accountable for content on their platforms.

Key Duties and Obligations under the IT Rules, 2021:

1. **Publication of Policies:** Intermediaries must publish their rules and regulations, privacy policy, and user agreement on their website/app, informing users about prohibited content and terms of service.
2. **Content Moderation (Prohibited Content):**
    - They must make reasonable efforts to cause users not to host, display, upload, modify, publish, transmit, store, update, or share any information that is prohibited (e.g., unlawful, harmful, harassing, defamatory, obscene, pornographic, pedophilic, invasive of privacy, hateful, racially/ethnically objectionable, relating to money laundering or gambling, infringing IP, misleading, impersonating, threatening unity/integrity/security of India, etc.).
    - **Automated Tools:** SSMIs are encouraged to use technology-based measures, including automated tools, for identifying certain types of content (e.g., child sexual abuse material, rape).
3. **Grievance Redressal Mechanism:**
    - All intermediaries must appoint a **Grievance Officer** who is a resident of India. The officer must acknowledge complaints within 24 hours and resolve them within 15 days.
    - **Specific Takedown Timelines:** For content depicting nudity, sexual acts, or impersonation (especially that which exposes the private area of any individual or depicts them in a sexual act), intermediaries must remove or disable access within **24 hours** of receiving a complaint.
4. **Traceability (for Significant Social Media Intermediaries offering messaging services):**

- SSMIs primarily offering messaging services (like WhatsApp) are required to enable the identification of the **first originator** of information on their platform, if required by a court order or an order from a competent authority. This is a highly debated provision due to its implications for end-to-end encryption and user privacy.

5. **Additional Obligations for Significant Social Media Intermediaries (SSMIs):**
   - Appoint a **Chief Compliance Officer** (liable in proceedings related to third-party content).
   - Appoint a **Nodal Contact Person** for 24x7 coordination with law enforcement agencies.
   - Publish a **monthly compliance report** detailing complaints received and actions taken.
   - Enable **voluntary user verification** mechanism.
6. **Retention of Information:** Intermediaries must preserve information and associated records of unlawful acts for at least **180 days** for investigation purposes.
7. **Assistance to Government Agencies:** Provide information or assistance to government agencies lawfully authorized for verification of identity, or for preventing, detecting, investigating, or prosecuting any offense, or for cybersecurity incidents, within **72 hours** of receiving a lawful order.
8. **User Notification:** Inform users at least once a year about their rules and regulations, privacy policy, and user agreement, and that non-compliance may lead to termination of access or content removal.

IV. Challenges and Debates Surrounding Intermediary Regulation

The regulation of intermediaries in India, especially with the IT Rules, 2021, has generated significant debate:

- **Balancing Freedom of Speech and Content Regulation:** Striking a balance between protecting freedom of expression and curbing harmful/illegal content is a perpetual challenge.
- **Over-Censorship/Over-Blocking:** Critics worry that stringent rules might lead intermediaries to proactively censor content to avoid liability, potentially chilling free speech.
- **Traceability vs. Privacy/Encryption:** The "first originator" rule for messaging apps has raised concerns about breaking end-to-end encryption and compromising user privacy.
- **Automated Filtering:** The reliance on automated tools for content moderation raises questions about accuracy, bias, and the potential for wrongful takedowns.
- **"Active" vs. "Passive" Intermediary:** The distinction between an intermediary merely hosting content (passive) and one actively involved in its creation or promotion (active) remains a complex area, often decided by courts on a case-by-case basis. If an intermediary is deemed "active," they lose safe harbor protection.
- **New Digital India Act:** The Indian government is in the process of formulating a new **Digital India Act (DIA)** to replace the IT Act, 2000. This new legislation is expected to further refine the regulatory framework for intermediaries, potentially introducing a risk-based approach to obligations and addressing emerging technologies like AI.

UNIT-III

UNIT - III: Overview of Rules Issued Under The It Act, 2000, Electronic Commerce, Electronic Contracts, Cyber Crimes, Cyber Frauds.

Overview of Rules Issued Under The It Act, 2000:

The Information Technology Act, 2000 (IT Act), as amended, is the foundational law for governing electronic transactions and cybercrime in India. While the Act itself lays down broad principles and offenses, the Central Government is empowered under Section 87 to make various rules to carry out the provisions of the Act. These rules provide the detailed procedures, standards, and guidelines for the implementation and enforcement of the IT Act.

Here's an overview of some of the most significant rules issued under the IT Act, 2000:

Information Technology (Certifying Authorities) Rules, 2000:

1**.Purpose:** These rules are fundamental for the legal recognition and regulation of Digital Signatures in India, which are crucial for e-commerce and secure electronic transactions.

- **Key Provisions:**
  - Establish the framework for the **Controller of Certifying Authorities (CCA)**, including its powers and functions.
  - Prescribe the qualifications, capital requirements, and other conditions for organizations to obtain a **license as a Certifying Authority (CA)**.
  - Detail the procedures for issuing, suspending, and revoking **Digital Signature Certificates (DSCs)**.
  - Specify the security procedures, audit requirements, and best practices that CAs must adhere to for ensuring the integrity and authenticity of digital signatures.
  -
  - Define the format and content of Digital Signature Certificates.

2. **Significance:** Ensures the trustworthiness and legal validity of electronic signatures, a cornerstone of digital governance and secure online dealings.
3. **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules):**
   - **Purpose:** These rules were framed to provide a legal framework for the protection of "sensitive personal data or information" collected, stored, processed, or handled by body corporates in India.
   - **Key Provisions:**
     - **Definition of Sensitive Personal Data or Information (SPDI):** Clearly defines what constitutes sensitive personal data, including passwords, financial information, health conditions, sexual orientation, biometrics, etc.
     - **Requirement for Privacy Policy:** Mandates that body corporates having SPDI must publish a clear privacy policy on their website, detailing the type of information collected, the purpose of collection, and security practices.
     - **Consent:** Requires explicit consent (in writing, fax, or email) from the information

provider before collecting or using their SPDI.

- **Reasonable Security Practices:** Obligates body corporates to implement "reasonable security practices and procedures" commensurate with international standards (like ISO 27001) to protect SPDI from unauthorized access, loss, disclosure, or alteration.
- **Grievance Redressal:** Requires the appointment of a Grievance Officer whose contact details must be published, to address grievances within one month.
- **Disclosure Restrictions:** Imposes restrictions on the disclosure of SPDI to third parties without consent, except in specific legal circumstances.

- **Significance:** These rules were India's primary data protection framework before the enactment of the Digital Personal Data Protection Act, 2023. While the DPDP Act now governs comprehensive data protection, the SPDI Rules provided essential guidelines for handling sensitive data for over a decade.

4. **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:**
   - **Purpose:** These are highly significant and often debated rules aimed at making social media platforms and other online intermediaries more accountable for content hosted on their platforms, and to regulate digital news publishers and OTT (Over-the-Top) streaming platforms.
   - **Key Provisions:**
     - **Due Diligence by Intermediaries:** Mandates "due diligence" requirements for intermediaries (e.g., social media companies, internet service providers). This includes publishing user agreements, privacy policies, and rules for content usage.
     - **Grievance Redressal Mechanism:** Requires intermediaries to establish a robust grievance redressal mechanism, including the appointment of a Grievance Officer residing in India, who must acknowledge complaints within 24 hours and resolve them within 15 days.
     - **Content Takedown:** Specifies timelines for removing unlawful content upon receiving a court order, government notification, or user complaint. Sexually explicit content, in particular, must be removed within 24 hours of a complaint.
     - **Traceability of Originator (for Significant Social Media Intermediaries):** For "significant social media intermediaries" (based on user numbers) providing messaging services, they must enable the identification of the "first originator" of a message for specific serious offenses, if required by a court order or competent authority. This is a highly contentious provision due to privacy concerns (e.g., end-to-end encryption).
     - **Additional Obligations for Significant Intermediaries:** These include appointing a Chief Compliance Officer, a Nodal Contact Person (for law enforcement coordination), and publishing monthly compliance reports.
     - **Digital Media Ethics Code:** Introduces a three-tier self-regulatory mechanism for digital news publishers and online curated content (OTT platforms), with increasing oversight from self-regulatory bodies and ultimately, the Ministry of Information

and Broadcasting. This includes adherence to a Code of Ethics and content classification.

- **Significance:** These rules represent a major attempt by the government to regulate the digital space, balance user freedom of speech with accountability, and provide a faster redressal mechanism for online harms.

5. **Information Technology (Electronic Service Delivery) Rules, 2011:**
   - **Purpose:** These rules aim to facilitate the electronic delivery of public services by the government to citizens, promoting e-governance.
   - **Key Provisions:**
     - Empower appropriate governments to authorize service providers for setting up, maintaining, and upgrading computerized facilities for electronic service delivery.
     - Specify how government services (like applications, certificates, licenses, payments) can be delivered electronically.
     - Aim to ensure transparency, efficiency, accountability, and reliability in the electronic delivery of such services.
   - **Significance:** Supports the Digital India initiative by providing the regulatory backbone for government services to go digital.

Other rules also exist or have existed, such as those governing Cyber Cafes (though less relevant now) and specific procedures for various aspects of the IT Act.

In essence, the IT Act, 2000, provides the legislative skeleton, and these various rules fill in the flesh, providing the detailed operational guidelines and regulatory mechanisms necessary for the effective functioning of India's digital ecosystem and enforcement of its cyber laws.

Electronic Commerce:

Electronic commerce, widely known as e-commerce, refers to the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. It encompasses a vast range of online business activities, from online retail shopping to electronic banking, digital product sales, and online marketplaces.

How E-commerce Works

At its core, e-commerce involves digital transactions facilitated by various technologies. A typical e-commerce transaction might involve:

1. Online Storefront/Platform: A website, mobile app, or online marketplace (like Amazon, Flipkart, eBay) where products/services are listed.
2. Product/Service Discovery: Customers browse, search, and discover items.
3. Order Placement: Customers add items to a virtual cart and proceed to checkout.
4. Payment Processing: Secure online payment gateways (credit/debit cards, UPI, net banking, digital wallets) facilitate the transaction.
5. Order Fulfillment: For physical goods, this involves inventory management, packaging, and shipping. For digital goods/services, it's typically instant delivery or access.
6. Customer Service: Online support, returns, and refunds.

Key Types of E-commerce Models:-

E-commerce is categorized based on the parties involved in the transaction:

1. Business-to-Consumer (B2C): This is the most common model, where businesses sell products or services directly to individual consumers.
    - Examples: Amazon, Flipkart, Myntra, Zomato, Netflix.
2. Business-to-Business (B2B): Transactions of goods and services conducted electronically between two businesses. This often involves wholesalers selling to retailers, manufacturers selling components to other manufacturers, or software companies selling enterprise solutions.
    - Examples: https://www.google.com/search?q=Alibaba.com, IndiaMART, SAP Ariba.
3. Consumer-to-Consumer (C2C): Consumers sell products or services directly to other consumers, usually through a third-party platform that facilitates the transaction.
    - Examples: eBay, OLX, Quikr, Facebook Marketplace.
4. Consumer-to-Business (C2B): Individuals offer their products or services to businesses. This often involves freelancers, consultants, or influencers selling their skills or services.
    - Examples: Upwork, Fiverr, stock photo websites where photographers sell images to businesses.
5. Business-to-Administration (B2A) / Business-to-Government (B2G): Electronic transactions between businesses and public administration/government entities. This includes government procurement, tenders, and services.
    - Examples: Government e-marketplace (GeM) in India.
6. Consumer-to-Administration (C2A) / Consumer-to-Government (C2G): Electronic transactions between individuals and public administration.
    - Examples: Filing taxes online, paying utility bills, applying for government services electronically.

Benefits of E-commerce

- Global Reach: Businesses can sell to customers anywhere in the world, transcending geographical limitations of a physical store.
- 24/7 Availability: Online stores are open around the clock, allowing customers to shop at their convenience.
- Lower Operating Costs: Compared to traditional brick-and-mortar stores, e-commerce businesses often have significantly lower overheads (no rent for physical space, fewer staff).
- Increased Sales & Revenue: Wider reach and constant availability can lead to higher sales volumes.
- Enhanced Customer Insights: E-commerce platforms allow for extensive data collection on customer behavior, preferences, and purchasing patterns, enabling personalized marketing and product development.
- Greater Product Variety: Online stores can offer a much wider range of products without physical display constraints.
- Convenience for Customers: Shoppers can browse and purchase from the comfort of their homes or on the go, saving time and effort.
- Easy Scalability: Online businesses can more easily scale up or down to meet demand fluctuations without needing to relocate or expand physical premises.
- Direct Customer Interaction: Many platforms facilitate direct communication between buyers and sellers, fostering better customer service and feedback.

Challenges of E-commerce:-

- Intense Competition: The low barrier to entry means a crowded marketplace, making it difficult for businesses to stand out.
- Cybersecurity & Fraud: E-commerce businesses are constant targets for cyberattacks, data breaches, and payment fraud, requiring robust security measures.
- Customer Trust & Returns: Building trust online can be challenging. High return rates (especially for fashion/apparel) can impact profitability.
- Logistics & Supply Chain Management: Efficient inventory management, warehousing, and timely delivery are critical and complex, especially for cross-border e-commerce.
- Payment Gateway Issues: Ensuring diverse, secure, and reliable payment options is crucial.
- Website Performance & User Experience: Slow loading times, complex navigation, or poor mobile responsiveness can lead to high cart abandonment rates.
- Customer Acquisition Cost (CAC): Attracting and retaining customers in a competitive online environment can be expensive due to marketing and advertising costs.
- Lack of Physical Interaction: Customers cannot physically inspect products, which can lead to dissatisfaction or returns.
- Technical Glitches: Downtime, bugs, or technical issues can directly impact sales and customer satisfaction.
- Regulatory Compliance: Navigating complex and evolving e-commerce laws (data protection, consumer rights, taxation) across different regions.

E-commerce Laws and Regulations in India:-

The e-commerce sector in India is governed by a blend of existing laws and specific rules, reflecting its rapid growth:

1. Information Technology Act, 2000 (IT Act): This is the primary legislation. It provides legal recognition for electronic transactions, digital signatures, and electronic records. It also addresses various cybercrimes relevant to e-commerce (e.g., hacking, data theft, cyber fraud).
2. Consumer Protection (E-Commerce) Rules, 2020: Issued under the Consumer Protection Act, 2019, these rules are specifically designed to protect consumers in e-commerce. Key provisions include:
    - Transparency: E-commerce entities must display detailed information about sellers, product prices, expiry dates, country of origin, and return/refund policies.
    - Grievance Redressal: Mandatory appointment of a Grievance Officer and establishment of a grievance redressal mechanism.
    - Prohibition of Unfair Trade Practices: Bans on misleading advertisements, manipulating product prices, and imposing cancellation charges without valid reason.
    - Flash Sales & Related Party Transactions: Restrictions on certain types of flash sales and prohibitions on "related party" sellers benefiting from preferential treatment on platforms.
3. Foreign Direct Investment (FDI) Policy: India's FDI policy regulates foreign investment in the e-commerce sector. Generally, 100% FDI is allowed in the marketplace model (where the platform acts as an intermediary), but FDI is prohibited in the inventory model (where the e-commerce entity owns the goods it sells directly in B2C).
4. Payment and Settlement Systems Act, 2007: Regulates payment systems in India, ensuring secure

and efficient electronic payment transactions for e-commerce. The RBI issues various guidelines under this Act for payment gateways and digital wallets.

5. Legal Metrology Act, 2009: Mandates specific declarations on pre-packaged commodities, including those sold online (e.g., net quantity, maximum retail price, date of manufacture/expiry, country of origin).
6. Intellectual Property Rights (IPR) Laws: Laws related to copyrights, trademarks, and patents are applicable to protect digital content, brand names, and product designs sold online, addressing issues like counterfeiting and copyright infringement.
7. Taxation Laws (GST, Income Tax): E-commerce transactions are subject to Goods and Services Tax (GST) and income tax as per standard Indian tax laws. Specific provisions for Tax Collected at Source (TCS) apply to e-commerce operators.
8. Digital Personal Data Protection Act, 2023: This landmark law (which has largely replaced parts of the IT Act and the SPDI Rules for data protection) governs the processing of digital personal data in India. It places strong obligations on e-commerce entities regarding data collection, consent, usage, storage, and security, with significant penalties for non-compliance.

E-commerce has profoundly transformed the retail landscape and consumer behavior in India, offering immense opportunities while necessitating a robust regulatory environment to ensure fair practices, consumer protection, and data security.

Electronic commerce, universally known as e-commerce, is the process of buying and selling goods and services, or the transmitting of funds or data, over an electronic network, predominantly the internet. It fundamentally transforms traditional commerce by leveraging digital technologies to facilitate transactions between parties.

How E-commerce Operates

E-commerce involves a series of interconnected digital processes:

1. Online Presence: Businesses establish an online storefront (website, mobile app) or utilize third-party marketplaces (e.g., Amazon, Flipkart) to display their products or services.
2. Customer Interaction: Consumers browse product catalogs, search for specific items, read reviews, and add desired items to a virtual shopping cart.
3. Secure Transactions: Upon checkout, integrated payment gateways (supporting credit/debit cards, UPI, net banking, digital wallets) securely process financial transactions.
4. Order Fulfillment: For physical goods, this involves inventory management, packaging, and shipping logistics. For digital products (e.g., software, e-books, streaming services), delivery is typically instantaneous via download or direct access.
5. Post-Purchase Support: E-commerce includes customer service channels for inquiries, returns, refunds, and technical support.

Key E-commerce Models

E-commerce is broadly categorized based on the parties involved in the transaction:

- **Business-to-Consumer (B2C):** This is the most common form, where businesses sell directly to individual end-users.
    - Examples: Online retailers like Amazon India, Myntra, Zomato (food delivery), Netflix **(streaming services).**
- **Business-to-Business (B2B):** Electronic transactions occur between two businesses. This includes

manufacturers selling to wholesalers, wholesalers selling to retailers, or software companies providing services to other enterprises.
    - Examples: https://www.google.com/search?q=Alibaba.com, IndiaMART, SAP Ariba.
- Consumer-to-Consumer (C2C): Individuals sell goods or services directly to other consumers, typically facilitated by a third-party platform.
    - Examples: eBay, OLX, Quikr, Facebook Marketplace.
- Consumer-to-Business (C2B): Individuals offer their products or services to businesses. This often involves freelancers, consultants, or content creators selling their skills or creations.
    - Examples: Upwork, Fiverr, stock photography websites.
- Business-to-Administration (B2A) / Business-to-Government (B2G): Electronic transactions between businesses and public administration or government entities, often related to procurement, tenders, or regulatory compliance.
    - Examples: Government e-Marketplace (GeM) in India.
- Consumer-to-Administration (C2A) / Consumer-to-Government (C2G): Electronic interactions and transactions between individuals and government bodies, such as online tax filing, bill payments, or application for public services.

E-commerce in India: Current Trends and Legal Landscape

India's e-commerce sector is booming, driven by increasing internet penetration, smartphone adoption, and government initiatives promoting digitalization.

Current Trends in India (as of mid-2025):

- Mobile Commerce (M-commerce) Dominance: A significant majority (over 70%) of e-commerce transactions in India occur via mobile devices, highlighting the importance of mobile-first strategies.
- Growth in Tier-2 & Tier-3 Cities: Demand from smaller cities and towns is a major growth driver, seeking convenience and wider product availability.
- Rise of Quick Commerce (Q-commerce): Companies like Blinkit and Zepto are fulfilling instant gratification needs by delivering groceries and essentials in under 30 minutes, a rapidly expanding segment.
- Social Commerce Integration: Social media platforms are increasingly becoming direct sales channels, with influencers driving purchases and live shopping gaining traction.
- Focus on Personalization and AI: E-commerce players are leveraging Artificial Intelligence (AI) and Machine Learning (ML) for personalized product recommendations, enhanced customer service (chatbots), and optimized operations.
- Sustainability and Health-Conscious Shopping: Growing consumer preference for eco-friendly products, organic skincare, and health & wellness items.
- Omnichannel Strategies: A blended approach integrating online and offline experiences (e.g., buying online, picking up in-store; AR/VR for virtual trials) is becoming the norm.
- Open Network for Digital Commerce (ONDC): A government-backed initiative aiming to democratize e-commerce by providing an open network protocol for buyers and sellers, challenging the dominance of large platforms and empowering small businesses.

Key Laws and Regulations in India (as of mid-2025):

1. Information Technology Act, 2000 (IT Act): The foundational law providing legal recognition to

electronic transactions, digital signatures, and electronic records. It also defines cybercrimes relevant to e-commerce (e.g., data theft, cyber fraud, hacking).

2. Consumer Protection (E-Commerce) Rules, 2020: Enacted under the Consumer Protection Act, 2019, these rules specifically address consumer rights in e-commerce. They mandate:
    - Transparency: Clear display of seller details, product information (including country of origin), and return/refund policies.
    - Grievance Redressal: Mandatory appointment of a Grievance Officer and a clear mechanism for complaint resolution.
    - Prohibition of Unfair Trade Practices: Bans misleading advertisements, price manipulation, and certain types of flash sales aimed at creating artificial scarcity.
    - "Related Party" Restrictions: Aim to prevent e-commerce platforms from giving preferential treatment to sellers in which they have a direct or indirect stake (though some proposed amendments in this area have been in flux).
3. Digital Personal Data Protection Act, 2023 (DPDP Act): This landmark law is the primary legislation for data protection in India. It places significant obligations on e-commerce entities regarding:
    - Consent: Obtaining explicit consent for processing personal data.
    - Purpose Limitation & Data Minimization: Collecting and using data only for specified, lawful purposes and only what is necessary.
    - Data Fiduciary Obligations: Ensuring accuracy, security, and integrity of personal data.
    - Data Breach Notification: Mandatory reporting of data breaches.
    - Cross-Border Data Transfer: Regulations on transferring personal data outside India.
    - Significant penalties for non-compliance.
4. Foreign Direct Investment (FDI) Policy: Regulates foreign investment in India's e-commerce sector. Generally, 100% FDI is permitted in the marketplace model (where the platform is an intermediary connecting buyers and sellers), but it is prohibited in the inventory-based model (where the e-commerce entity owns the goods it sells directly in B2C).
5. Payment and Settlement Systems Act, 2007: Governs digital payment systems, with the Reserve Bank of India (RBI) issuing regulations for payment gateways, digital wallets, and other electronic payment mechanisms used in e-commerce.
6. Goods and Services Tax (GST) Act, 2017: E-commerce transactions are fully integrated into the GST framework, including provisions for Tax Collected at Source (TCS) by e-commerce operators.
7. Legal Metrology (Packaged Commodities) Rules, 2011: Requires e-commerce entities to display mandatory declarations (e.g., MRP, net quantity, country of origin) for pre-packaged commodities sold online.

The Indian e-commerce landscape is dynamic, with continuous evolution in technology, consumer behavior, and regulatory frameworks. The focus remains on fostering growth while ensuring consumer protection, fair competition, and data security.

Electronic Contracts:-

Electronic contracts, often referred to as e-contracts or digital contracts, are agreements formed, executed, and enforced through electronic means, without the need for physical paper documentation. They are a

cornerstone of modern digital commerce and transactions, enabling speed, efficiency, and convenience.

How Electronic Contracts are Formed

E-contracts are formed when parties express their offer and acceptance through electronic communication. Common methods include:

- **Click-wrap Agreements:** The most prevalent type, where users explicitly agree to terms and conditions by clicking an "I Accept" or "I Agree" button or checking a box on a website or software interface. This is common for software licenses, online service agreements, and e-commerce checkouts.
- **Browse-wrap Agreements:** Terms and conditions are made available via a hyperlink on a website (e.g., in the footer), and acceptance is inferred from the user's continued use of the website. These are generally considered less enforceable than click-wrap agreements, as explicit consent is not obtained.
- **Email Agreements:** Contracts formed through a series of email exchanges where parties negotiate terms and eventually signify their offer and acceptance via email.
- **Electronic Signatures on Digital Documents:** Parties affix electronic signatures (including digital signatures) to electronic documents (e.g., PDFs) using specialized software or platforms.
- **Online Forms/Tailored Agreements:** Users fill out and electronically sign custom forms or agreements hosted on web portals, such as for online loan applications, insurance policies, or tenancy agreements.
- **Through Messaging Apps:** In some cases, courts have recognized agreements formed through exchanges on messaging apps like WhatsApp or Telegram, provided there is clear evidence of offer, acceptance, and intent to create legal relations.

Legal Validity of Electronic Contracts in India

In India, the legal validity and enforceability of electronic contracts are primarily derived from a combination of the **Indian Contract Act, 1872** and the **Information Technology Act, 2000 (IT Act)**.

1. **Indian Contract Act, 1872:**
    - The fundamental principles governing all contracts in India are laid down in this Act. For an e-contract to be legally valid, it must satisfy all the essential elements of a valid contract as per Section 10 of the Indian Contract Act:
        - Offer and Acceptance: There must be a clear proposal by one party and an unequivocal acceptance by the other. This can happen electronically.
        - Lawful Consideration: Something of value exchanged between the parties.
        - Free Consent: The consent of the parties must be genuine and not induced by coercion, undue influence, fraud, misrepresentation, or mistake.
        - Competent Parties: The parties must be of the age of majority (18 years), of sound mind, and not disqualified by any law from contracting.
        - Lawful Object: The purpose of the contract must be legal and not against public policy.
        - Intention to Create Legal Relations: The parties must intend their agreement to be legally binding.
        - Certainty and Possibility of Performance: The terms must be clear and the agreement capable of being performed.

2. **Information Technology Act, 2000 (IT Act):**
    - The IT Act provides the specific legal framework for electronic transactions and records. It plays a crucial role in validating e-contracts by addressing the electronic format:
        - **Section 4 (Legal Recognition of Electronic Records):** States that where any law requires information to be in written or typewritten form, that requirement is satisfied if it is made available in an electronic form.
        - **Section 5 (Legal Recognition of Electronic Signatures):** Grants legal recognition to electronic signatures (including Digital Signatures) affixed in the manner prescribed by the Central Government, equating them to handwritten signatures.
        - **Section 10A (Validity of Contracts formed through Electronic Means):** This is the most direct and crucial provision. It explicitly states: "Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose." This effectively removes any doubt about the legal validity of contracts solely because they are electronic.
        - **Section 65B (Admissibility of Electronic Records):** Outlines the conditions under which electronic records can be admitted as evidence in court, ensuring that e-contracts can be presented as proof in legal proceedings.

Types of Electronic Signatures in India

The IT Act, 2000 recognizes various electronic signatures:

- **Digital Signatures (DSC):** These are considered "secure electronic signatures" and are based on asymmetric crypto systems and hash functions. They require a Digital Signature Certificate issued by a licensed Certifying Authority (CA) in India (regulated by the Controller of Certifying Authorities - CCA). DSCs offer a high level of security and authenticity.
- **Electronic Signatures (E-Sign):** Introduced in 2008 amendments, this broader term covers various electronic authentication techniques. E-Sign is an online electronic signature service that facilitates signing of a document digitally using Aadhaar e-KYC services. It offers a simpler way to sign documents compared to DSCs.

Importance of Stamp Duty

While e-contracts are legally valid, they still generally require the payment of **stamp duty** to be admissible as evidence in Indian courts. Many states in India have introduced e-stamping facilities, allowing the stamp duty to be paid digitally and an electronic stamp certificate to be generated and attached to the e-contract. The amount of stamp duty varies based on the nature of the agreement and state laws.

Documents Not Permitted as E-contracts

The First Schedule of the IT Act, 2000, as amended, specifies certain documents that *cannot* be executed electronically and still require a physical form for validity:

- Negotiable Instruments (other than a cheque)
- Powers of Attorney
- Trusts

- Wills and any other testamentary disposition
- Any contract for the sale or conveyance of immovable property or any interest in such property (though there has been some debate and amendments here, physical registration of property documents remains generally mandatory).

Challenges and Judicial Precedents

Despite the legal framework, certain challenges remain:

- **Jurisdiction:** Determining the appropriate jurisdiction for disputes, especially in cross-border e-contracts, can be complex.
- **Authenticity and Attribution:** While electronic signatures aid this, proving the identity of the signer and ensuring the integrity of the electronic record can sometimes be challenging.
- **Negotiation in Standard Form Contracts:** Many e-contracts (like click-wrap) are "take-it-or-leave-it" agreements, with no scope for negotiation. Courts generally uphold these unless they are unconscionable or involve significant power imbalances.

Key Judicial Precedents:

- **Trimex International FZE Ltd. v. Vedanta Aluminium Ltd. (2010):** The Supreme Court of India notably upheld the validity of a contract formed through a series of email exchanges, emphasizing that an agreement concluded orally or in writing (including electronic form) is legally enforceable if the essential elements of a contract are met.
- Various High Courts have also reiterated the validity of electronic records and communications as evidence under Section 65B of the Indian Evidence Act, 1872.

In conclusion, electronic contracts are fully recognized and enforceable in India, provided they comply with the core principles of the Indian Contract Act and the specific provisions of the Information Technology Act. They are integral to the functioning of modern business and everyday digital interactions.

Cyber Crimes:

Cybercrime refers to any criminal activity that involves a computer, computer network, or networked device. It can be categorized into crimes where the computer is the *tool* to commit the offense (e.g., cyber fraud), and crimes where the computer is the *target* of the offense (e.g., hacking, malware attacks). With the pervasive use of the internet and digital technologies, cybercrime has become a significant global threat, causing immense financial losses, reputational damage, and psychological distress.

Categories and Common Types of Cybercrimes

Cybercrimes can be broadly classified into different categories, though many offenses often overlap:

I. Crimes Against Individuals (Targeting People):

1. **Cyberstalking and Online Harassment:** Repeated unwanted online contact, threats, monitoring online activity, or spreading false information to distress or intimidate a victim. (e.g., sending repeated abusive messages, creating fake profiles to torment someone).

2. **Cyberbullying:** The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. While not explicitly defined as a separate crime in India, it's addressed under various laws.
3. **Online Defamation:** Harming someone's reputation by publishing false and malicious statements about them on the internet (e.g., through social media, blogs, or websites).
4. **Doxing:** Publishing private or identifying information about an individual on the internet, typically without their consent, with malicious intent.
5. **Online Impersonation/Identity Theft:** Stealing and using another person's personal information (e.g., passwords, Aadhaar numbers, credit card details) to commit fraud, gain access to accounts, or create fake online profiles.
6. **Sextortion:** Blackmailing individuals by threatening to publish sexually explicit images or videos of them unless a ransom (often money or more explicit content) is paid.
7. **Phishing/Smishing/Vishing:** Deceptive attempts to trick individuals into revealing sensitive information (passwords, bank details) by posing as a trustworthy entity via fake emails (phishing), SMS (smishing), or phone calls (vishing).
8. **Job Scams/Online Frauds:** Deceiving individuals with fake job offers, lottery wins, investment schemes, or romantic relationships (romance scams) to extract money or personal information.
9. **Online Child Sexual Abuse Material (CSAM) / Child Pornography:** Production, distribution, or accessing of sexually explicit material involving minors. This is a severe crime globally.
10. **Revenge Pornography / Non-Consensual Intimate Image (NCII) Sharing:** Publishing or sharing private sexual images or videos of someone without their consent, often after a relationship ends.

II. Crimes Against Property (Targeting Systems/Data):

1. **Hacking / Unauthorized Access:** Gaining unauthorized access to computer systems, networks, websites, or data. This can be for theft, sabotage, or mere mischief.
2. **Malware Attacks:**
    - **Viruses & Worms:** Malicious programs that replicate and spread, damaging data or disrupting system operations.
    - **Trojans:** Malware disguised as legitimate software that, once installed, creates backdoors for attackers.
    - **Ransomware:** Encrypts a victim's files and demands a ransom payment (often in cryptocurrency) for their release.
    - **Spyware:** Secretly monitors computer activity and collects personal information.
    - **Adware:** Displays unwanted advertisements.
3. **Data Theft / Data Breach:** Unauthorized access, acquisition, or transmission of sensitive personal or organizational data.
4. **Distributed Denial of Service (DDoS) Attacks:** Overwhelming a target server or network with a flood of internet traffic to disrupt its normal functioning, making services unavailable to legitimate users.
5. **Web Jacking:** Taking forceful control of another person's website.

6. **Intellectual Property Rights (IPR) Violations:** Software piracy, copyright infringement (e.g., illegal streaming, unauthorized distribution of copyrighted content), trademark violations, and theft of trade secrets online.
7. **Cryptojacking:** Secretly using a victim's computer processing power to mine cryptocurrency without their consent.

III. Crimes Against Government/Society (Broader Impact):

1. **Cyber Terrorism:** Using the internet and digital systems to carry out acts of terrorism, such as disrupting critical infrastructure (power grids, financial systems), spreading propaganda, or coordinating attacks.
2. **Cyber Warfare:** Nation-state sponsored cyberattacks targeting another country's critical infrastructure, military systems, or government networks.
3. **Online Drug Trafficking/Illegal Trade:** Using the dark web or encrypted messaging apps to facilitate the illegal buying and selling of drugs, weapons, or other illicit goods.
4. **Financial Frauds:** Broader category of scams aimed at illegally obtaining money through digital means (e.g., credit card fraud, online banking fraud, investment scams).
5. **Phishing for Government Credentials:** Attempts to steal login credentials for government systems.

Legal Framework for Cybercrimes in India

India primarily addresses cybercrimes through two main statutes:

1. **The Information Technology Act, 2000 (IT Act) & its Amendments:**
    - This is the principal legislation dedicated to electronic commerce and cybercrime in India.
    - **Section 43:** Penalty and compensation for damage to computer systems, data, or networks (e.g., unauthorized access, introducing viruses, causing disruption).
    - **Section 65:** Tampering with computer source documents.
    - **Section 66:** Computer-related offenses (e.g., hacking, causing wrongful loss or damage to data).
    - **Section 66B:** Dishonestly receiving stolen computer resources or communication devices.
    - **Section 66C:** Identity theft (using another person's password, digital signature, or unique identification fraudulently).
    - **Section 66D:** Cheating by personation using computer resources.
    - **Section 66E:** Punishment for violation of privacy (publishing or transmitting images of a private area without consent – directly addresses "revenge porn").
    - **Section 66F:** Cyber Terrorism (acts threatening India's unity, integrity, security, or sovereignty through cyber means).
    - **Section 67:** Publishing or transmitting obscene material in electronic form.
    - **Section 67A:** Publishing or transmitting material containing sexually explicit acts in electronic form.

- **Section 67B:** Publishing or transmitting material depicting children in sexually explicit acts (child pornography).
- **Section 69:** Power to issue directions for interception or monitoring or decryption of any information.
- **Section 69A:** Power to issue directions for blocking for public access of any information through any computer resource.
- **Section 72:** Breach of confidentiality and privacy.
- **Section 74:** Publication for fraudulent purpose.

2. **Indian Penal Code, 1860 (IPC):**
   - Many traditional crimes, when committed using a computer or the internet, are also covered by relevant sections of the IPC. The IT Act often complements these:
   - **Section 354D:** Stalking (specifically includes online monitoring or contacting despite disinterest).
   - **Section 420:** Cheating (often invoked in online fraud cases).
   - **Section 463-471:** Forgery (creating fake electronic documents or digital signatures).
   - **Section 499/500:** Defamation (online slander or libel).
   - **Section 503/506/507:** Criminal Intimidation (online threats, including anonymous ones).
   - **Section 509:** Word, gesture, or act intended to insult the modesty of a woman (often used for online sexual harassment).
   - **Section 292/293/294:** Obscenity (public display of obscene material, including online).
3. **Protection of Children from Sexual Offences (POCSO) Act, 2012:**
   - Crucial for cases involving child victims of online sexual abuse, exploitation, or grooming. It provides stricter penalties than the IT Act for offenses related to CSAM.
4. **Digital Personal Data Protection Act, 2023 (DPDP Act):**
   - While not strictly a cybercrime law, it imposes significant obligations on organizations handling personal data. Violations, especially data breaches due to negligence, can lead to substantial penalties, thereby deterring a form of "cyber harm" that often precedes or enables other cybercrimes.

Reporting Cybercrimes in India

- **National Cybercrime Reporting Portal:** `www.cybercrime.gov.in` (launched by the Ministry of Home Affairs). This is the central portal for reporting all types of cybercrimes.
- **Police Cyber Cells:** Most major cities and states have dedicated Cyber Crime Cells within their police departments.
- **Local Police Stations:** For general cybercrimes, an FIR (First Information Report) can be lodged at any local police station.

Cybercrime is a dynamic and evolving threat. Staying informed about the latest scams, practicing good cyber hygiene, and understanding the legal recourse available are essential for digital safety.

Cyber Frauds:

Cyber fraud, a pervasive subset of cybercrime, involves the use of digital technology to deceive individuals or organizations for financial gain. These frauds leverage the internet, email, mobile phones, and various online platforms to trick victims into revealing sensitive information, making unauthorized payments, or falling for deceptive schemes.

In India, with its rapidly expanding digital economy and internet user base, cyber frauds are a significant concern, leading to substantial financial losses for individuals and businesses alike.

Common Types of Cyber Frauds in India:

1. **Phishing/Smishing/Vishing:**
    - **Phishing:** Sending fraudulent emails that appear to be from legitimate organizations (banks, government agencies, popular services) to trick recipients into revealing personal details like passwords, credit card numbers, or OTPs.
    - **Smishing:** The SMS equivalent of phishing, where fraudulent text messages are used.
    - **Vishing:** Voice phishing, where fraudsters make deceptive phone calls, often posing as bank representatives, tech support, or government officials, to extract sensitive information.
    - **Modus Operandi:** Creating a sense of urgency or fear (e.g., "Your account will be suspended!"), offering tempting rewards ("You've won a lottery!"), or providing fake technical support.
2. **Online Banking Fraud:**
    - **Malware/Keyloggers:** Installing malicious software on a victim's device to capture banking credentials.
    - **Man-in-the-Middle (MitM) Attacks:** Intercepting communications between a user and their bank's website to steal or alter data.
    - **Account Takeover (ATO):** Gaining unauthorized access to a victim's online banking account through stolen credentials (often obtained via phishing or credential stuffing) to initiate fraudulent transactions.
    - **SIM Swap Fraud:** Fraudsters illegally obtain a new SIM card for a victim's registered mobile number, allowing them to receive OTPs and bypass two-factor authentication to access bank accounts and digital wallets.
3. **Credit/Debit Card Fraud:**
    - **Skimming:** Using devices installed at ATMs or POS terminals to illegally copy card data.
    - **Online Card Not Present (CNP) Fraud:** Using stolen card details for online purchases without the physical card.
    - **Phishing/Vishing for Card Details:** Directly tricking victims into divulging card numbers, CVV, expiry dates, and OTPs.
4. **UPI (Unified Payments Interface) Fraud:**
    - **Request Money Scams:** Fraudsters send "collect requests" on UPI apps, tricking users into entering their PIN to "receive" money, which actually authorizes a payment *from* their account.

- **QR Code Scams:** Generating fake QR codes that, when scanned, initiate a payment from the victim's account instead of facilitating a transaction for goods/services.
- **OTP Sharing:** Tricking users into sharing UPI PINs or OTPs through various social engineering tactics.

5. **Online Shopping Fraud / E-commerce Fraud:**
   - **Fake Websites:** Creating highly convincing but fake e-commerce websites to lure customers into making purchases for non-existent products or to steal their financial details.
   - **Non-Delivery Scams:** Accepting payment for goods that are never delivered.
   - **Counterfeit Products:** Selling fake or substandard products disguised as genuine items.
   - **Advance Fee Scams:** Demanding upfront payments for products/services that are never provided.
6. **Job Scams / Employment Fraud:**
   - Offering fake job opportunities (often overseas or with incredibly high salaries) to extract "processing fees," "training costs," or personal information from desperate job seekers.
7. **Loan Fraud:**
   - Offering instant loans with no credit checks for an upfront "processing fee," only to disappear after receiving the money.
   - Demanding "insurance" or "GST" payments before disbursing the loan, which never arrives.
8. **Investment Scams:**
   - **Ponzi/Pyramid Schemes:** Promising unusually high returns on investments with little or no risk, using funds from new investors to pay earlier ones.
   - **Fake Trading Platforms:** Creating elaborate fake platforms for cryptocurrency, forex, or stock trading to lure victims into investing money that is then siphoned off.
9. **Social Media Frauds:**
   - **Impersonation:** Creating fake profiles of friends, relatives, or celebrities to solicit money or personal information.
   - **Lottery/Prize Scams:** Informing users they've won a lottery or contest, then demanding a "processing fee" or "tax" to release the non-existent prize.
   - **Romance Scams:** Building emotional relationships with victims online to eventually ask for money for fake emergencies or travel expenses.
10. **Tech Support Scams:**
    - Fraudsters call or display pop-up messages claiming to be from reputable tech companies (e.g., Microsoft) and trick victims into giving remote access to their computers, often leading to installation of malware or demanding payment for unnecessary "fixes."
11. **Business Email Compromise (BEC):**
    - Highly sophisticated scams targeting businesses, where fraudsters impersonate executives or trusted vendors to trick employees into transferring funds or sensitive data to fraudulent accounts.

Impact of Cyber Frauds:

- **Financial Losses:** The most direct and obvious impact, ranging from small amounts to significant life savings.
- **Identity Theft:** Stolen personal data can be used for further frauds, opening fake accounts, or taking out loans in the victim's name.
- **Emotional Trauma & Stress:** Victims often experience feelings of betrayal, anger, embarrassment, and helplessness.
- **Reputational Damage:** For businesses, a cyber fraud incident can lead to a loss of customer trust, negative publicity, and damage to brand reputation.
- **Operational Disruption:** Businesses can face significant downtime and operational challenges following a cyber fraud or data breach.
- **Legal & Regulatory Consequences:** For businesses, non-compliance with data protection laws or negligence leading to fraud can result in heavy fines and legal action.
- **Increased Security Costs:** Both individuals and businesses may have to invest more in cybersecurity measures after being targeted.

Prevention and Safeguards:

- **Be Skeptical of Unsolicited Communications:** Never click on suspicious links, open unknown attachments, or respond to messages/calls requesting personal or financial details. Always verify the sender's identity through official channels.
- **Verify Website Authenticity:** Always check for "HTTPS" and the padlock icon in the URL bar, especially before making payments or entering sensitive information. Type URLs directly instead of clicking links.
- **Use Strong, Unique Passwords & MFA:** Use complex, unique passwords for all accounts and enable Multi-Factor Authentication (MFA) wherever possible.
- **Keep Software Updated:** Regularly update your operating system, web browsers, and antivirus software to patch known vulnerabilities.
- **Install Reputable Antivirus/Anti-Malware:** Use comprehensive internet security suites on all devices.
- **Do Not Share OTPs/PINs:** Your bank or any legitimate entity will *never* ask for your OTP, PIN, CVV, or full card number over the phone, email, or SMS.
- **Beware of "Too Good To Be True" Offers:** If an offer seems unbelievably good (e.g., huge lottery wins for a small fee, extremely high returns on investments), it's likely a scam.
- **Review Account Statements:** Regularly check bank, credit card, and digital wallet statements for any suspicious or unauthorized transactions.
- **Secure Public Wi-Fi:** Avoid conducting sensitive transactions on public Wi-Fi. If necessary, use a Virtual Private Network (VPN).
- **Limit Personal Information Sharing Online:** Be cautious about what personal details you share on social media or public platforms, as this information can be used by fraudsters.
- **Educate Yourself:** Stay informed about the latest cyber fraud techniques and awareness campaigns by government and financial institutions.

How to Report Cyber Fraud in India:

If you are a victim of cyber fraud in India, immediate action is crucial to maximize the chances of recovering funds and catching the perpetrators:

1. **Contact Your Bank/Financial Institution Immediately:**
    - Report the fraudulent transaction to your bank, credit card company, or digital wallet provider.
    - Request them to block your card/account and reverse the transaction. Time is of the essence here.
2. **File a Complaint on the National Cybercrime Reporting Portal:**
    - Visit the official portal: **www.cybercrime.gov.in**
    - Click on "Report Cyber Crime" and then "File a Complaint."
    - Provide all necessary details: your personal details, incident details (what happened, when, how), transaction details (if money was lost, including bank account, UPI ID, transaction ID, date, and time), and any suspect details you might have.
    - Upload supporting documents/evidence (screenshots, SMS, emails).
    - You will receive an acknowledgement number for tracking your complaint.
3. **Call the Cybercrime Helpline:**
    - Dial **1930** (a dedicated cybercrime hotline). This number is operational to report financial frauds and will often guide you through the process of freezing the fraudulent transaction if reported quickly.
4. **Lodge a Police Complaint (FIR):**
    - If the fraud involves significant loss or other serious criminal elements, consider lodging a First Information Report (FIR) at your local police station or dedicated Cyber Cell.

By understanding the types of cyber frauds and adopting proactive prevention measures, individuals and businesses can significantly reduce their vulnerability to these growing digital threats.

your roots to success...

UNIT-IV

Regulatory Authorities

Regulatory Authorities: Department of Electronics and Information Technology, Controller of Certifying Authorities (CCA), Cyber Appellate Tribuna, Indian Computer Emergency Response Team (ICERT), Cloud Computing, Case Laws.

Department of Electronics and Information Technology:

1. The functions of the Department of Electronics and Information Technology, Ministry of Communications & Information Technology, Government of India are as follows –
2. Policy matters relating to Information Technology, Electronics and Internet.
3. Initiatives for development of Hardware / Software industry including knowledge based enterprises, measures for promoting Information Technology exports and competitiveness of the industry.
4. Promotion of Information Technology and Information Technology enabled services and Internet.
5. Assistance to other departments in the promotion of E-Governance, E-Infrastructure, E-Medicine, E-Commerce, etc.
6. Promotion of Information Technology education and Information Technology-based education.
7. Matters relating to Cyber Laws, administration of the Information Technology Act. 2000 (21 of 2000) and other Information Technology related laws.
8. Matters relating to promotion and manufacturing of Semiconductor Devices in the country.
9. Interaction in Information Technology related matters with international agencies and bodies.
10. Initiative on bridging the Digital Divide, Matters relating to Media Lab Asia.

Controller of Certifying Authorities (CCA):

The Controller of Certifying Authorities (CCA) is a regulatory body in India under the Ministry of Electronics and Information Technology (MeitY). It was established under the Information Technology Act, 2000, to regulate the issuance of digital signatures and public key infrastructure (PKI) in the country.

Key Functions of CCA:

- Licensing and Regulation of Certifying Authorities (CAs)

a. Grants licenses to Certifying Authorities (CAs) to issue Digital Signature Certificates (DSCs).
b. Ensures that CAs comply with legal and technical requirements.
c. Conducts audits and security checks on CAs.

- Root Certifying Authority of India (RCAI)

a. Operates the Root Certifying Authority of India (RCAI), which digitally signs and certifies the public keys of licensed CAs.
b. Ensures a trusted digital certification framework in India.

- Ensuring Secure Digital Transactions

a. Promotes Digital Signature Certificates (DSCs) for secure authentication in online transactions.
b. Enables secure e-governance, e-commerce, e-tendering, and financial transactions.

- Compliance and Enforcement

a. Enforces Information Technology (Certifying Authorities) Rules, 2000.
b. Ensures that CAs follow cryptographic security standards and best practices.

- Digital Signature Standards and Guidelines

a. Specifies the standards for cryptographic algorithms and security infrastructure for digital signatures.
b. Works with international cyber security agencies to enhance security measures.

Root Certifying Authority of India (RCAI)

The Root Certifying Authority of India (RCAI) is managed by the CCA and serves as the apex authority for issuing and verifying public key certificates. It ensures the interoperability, authenticity, and integrity of digital signatures in India.

List of Licensed Certifying Authorities (CAs) in India

The CCA licenses private and government organizations to issue digital certificates. Some of the leading licensed Certifying Authorities in India include:

- eMudhra Limited
- (n)Code Solutions (GNFC)
- Sify Technologies
- National Informatics Centre (NIC CA)
- IDRBT Certifying Authority
- Capricorn CA

These CAs provide Digital Signature Certificates (DSCs) for individuals, businesses, and government organizations for use in e-filing, GST filing, e-tendering, and online banking.

Importance of CCA in Digital India

- Supports Digital India initiatives by ensuring secure online transactions.
- Prevents cyber fraud by authenticating electronic documents.
- Facilitates e-Governance, online tax filing, and secure communication.

Cyber Appellate Tribuna:

The Cyber Appellate Tribunal (CyAT) was a specialized tribunal established under the Information Technology Act, 2000 to handle appeals against decisions of the Adjudicating Officer related to cyber crimes and electronic commerce disputes in India. It was the first of its kind in the country, ensuring justice in cyber-related cases.

Key Functions of the Cyber Appellate Tribunal

1. **Hearing Appeals:**
   - CyAT heard appeals against orders passed by the Adjudicating Officer under the IT Act, 2000.
   - Cases included cyber fraud, hacking, data breaches, and financial cyber crimes.
2. **Jurisdiction & Authority:**
   - Had the power to overrule, modify, or uphold decisions made by the Adjudicating Officer.
   - Could summon evidence, examine witnesses, and pass legal judgments.
3. **Protecting Digital Rights:**
   - Helped individuals and businesses seek justice for cyber fraud, online contract

violations, and IT-related disputes.

4. **Encouraging Cybersecurity & Compliance:**
    - Ensured that companies followed IT security standards and protected user data.

Establishment and Purpose

The Cyber Appellate Tribunal (CyAT) was set up under Section 48 of the IT Act, 2000 to handle appeals against decisions made by the Adjudicating Officer under the same Act.

- **Why Was CyAT Established?**

- To provide a specialized forum for resolving cyber disputes.
- To reduce the burden on traditional courts in handling cybercrime cases.
- To ensure timely resolution of IT-related disputes in India.

- **Jurisdiction and Powers**

The tribunal had the authority to:

1. Hear appeals against orders passed by the Adjudicating Officer.
2. Overturn, modify, or uphold the decisions of lower authorities.
3. Summon witnesses and demand evidence in cyber-related cases.
4. Impose penalties and fines in cases of IT Act violations.
5. Provide legal relief to individuals or companies affected by cyber fraud or data breaches

Types of CasesHandled

- Hacking and unauthorized access to computer systems.
- Online identity theft and phishing scams.
- Cyber fraud, financial fraud, and online scams.
- Data theft and unauthorized data sharing.
- E-commerce disputes related to digital signatures and contracts.

Structure of the Cyber Appellate Tribunal

The Cya consisted of:

- Chairperson: A retired judge of the Supreme Court or High Court was appointed as the head of the tribunal.
- Members: Legal and technical experts assisted in reviewing cyber law cases.
- Registrar and Staff: Administrative and legal professionals helped in case processing and documentation.

Appeal Process in CyAT

Step 1: Filing an Appeal

- If an individual or organization was dissatisfied with the decision of the Adjudicating Officer, they could file an appeal with the Cyber Appellate Tribunal.

Step 2: Case Hearing

- The tribunal reviewed evidence, heard arguments, and analyzed digital records.

Step 3: Judgment and Relief

- The tribunal issued binding decisions, which could include fines, penalties, or other legal remedies.

Step 4: Further Appeal to the High Court

- If a party was not satisfied with the tribunal's decision, they could appeal to the High Court within 60 days of the judgment.

Where Are Cyber Appeals Now Heard?

After the abolition of CyAT, cyber-related appeals are handled by:

- Telecom Disputes Settlement and Appellate Tribunal (TDSAT)
- High Courts (in some cases)

Indian Computer Emergency Response Team (ICERT):

The correct and official name is **Indian Computer Emergency Response Team (CERT-In)**. While "ICERT" might be used informally or as a shorthand, the recognized acronym is CERT-In.

CERT-In is a crucial government organization under the **Ministry of Electronics and Information Technology (MeitY)**, Government of India. It was established in January 2004 under the Information Technology Act, 2000 (Section 70B), and serves as the national nodal agency for responding to computer security incidents.

Key functions and responsibilities of CERT-In include:

- **Collection, Analysis, and Dissemination of Information:** Gathering, analyzing, and sharing information on cyber incidents.
- **Forecasts and Alerts:** Providing forecasts and alerts on cybersecurity incidents and potential threats.
- **Emergency Measures:** Implementing emergency measures for handling cybersecurity incidents.
- **Coordination:** Coordinating cyber incident response activities across various sectors in India.
- **Issuance of Guidelines and Advisories:** Publishing guidelines, advisories, vulnerability notes, and whitepapers related to information security practices, procedures, prevention, response, and reporting of cyber incidents.
- **Cybersecurity Audits:** Empaneling and overseeing IT security auditing organizations to conduct vulnerability assessments and penetration testing for government and critical infrastructure organizations.
- **International Coordination:** Collaborating with international CERTs and participating in global forums to share information, coordinate responses, and build capacity in cybersecurity.
- **Capacity Building:** Conducting training programs and workshops to enhance cybersecurity awareness and skills.
- **Vulnerability Disclosure and Coordination:** Acting as a CVE Numbering Authority (CNA) for vulnerabilities impacting products designed, developed, and manufactured in India.

In essence, CERT-In acts as India's national incident response center, working proactively and reactively to secure Indian cyberspace and build a safe and trusted digital ecosystem for its citizens.

Cloud Computing:

Cloud computing is a revolutionary paradigm that delivers on-demand computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud"). Instead of owning and maintaining your own computing infrastructure, you can access these

services from a third-party cloud provider and pay only for what you use, much like a utility service.

How it Works

At its core, cloud computing involves a vast network of remote servers hosted on the internet and designed to store and manage data, run applications, and deliver content or services. When you use cloud computing, you're essentially accessing these resources over the internet, rather than having them physically located on your premises.

Key Characteristics of Cloud Computing

- **On-demand self-service:** Users can provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access:** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource pooling:** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer.

Cloud Deployment Models

Cloud services can be deployed in various ways:

- **Public Cloud:** Owned and operated by a third-party cloud service provider (e.g., Google Cloud, Amazon Web Services (AWS), Microsoft Azure). All hardware, software, and other supporting infrastructure are owned and managed by the cloud provider. Users access services and manage accounts using a web browser.
- **Private Cloud:** Cloud computing resources used exclusively by a single business or organization. A private cloud can be physically located on the company's onsite data center or hosted by a third-party service provider. It offers greater control, security, and customization.
- **Hybrid Cloud:** Combines public and private clouds, allowing data and applications to be shared between them. This offers greater flexibility, more deployment options, and helps optimize existing infrastructure, security, and compliance.
- **Community Cloud:** A collaborative infrastructure shared by several organizations from a specific community with shared concerns (e.g., security requirements, compliance, jurisdiction).

Cloud Service Models

Cloud computing offers different levels of abstraction and control:

- **Infrastructure as a Service (IaaS):** Provides on-demand access to fundamental IT infrastructure services, including compute (virtual machines), storage, networking, and virtualization. You manage the operating system, applications, and data, while the provider manages the underlying infrastructure.

- **Examples:** Amazon EC2, Google Compute Engine, Microsoft Azure Virtual Machines.

- **Platform as a Service (PaaS):** Delivers and manages hardware and software resources for developing, testing, delivering, and managing cloud applications. It provides a complete development environment, allowing developers to focus on writing code without worrying about the underlying infrastructure.
  - **Examples:** AWS Elastic Beanstalk, Google App Engine, Salesforce Platform.
- **Software as a Service (SaaS):** Delivers software applications over the internet, on demand, and typically on a subscription basis. The cloud provider hosts and manages the software application and underlying infrastructure, handling maintenance, upgrades, and security patching. Users simply access the application through a web browser or client.
  - **Examples:** Gmail, Salesforce, Microsoft 365, Dropbox, Zoom.
- **Serverless Computing (Function as a Service - FaaS):** A newer model that allows developers to build and run application functionalities without provisioning or managing servers. The cloud provider automatically manages the underlying infrastructure, scaling resources as needed for each function execution.
  - **Examples:** AWS Lambda, Google Cloud Functions, Azure Functions.

Benefits of Cloud Computing

- **Cost Savings:** Reduces capital expenditures (no need to buy expensive hardware/software) and allows for a "pay-as-you-go" operational expense model, paying only for what you use.
- **Scalability and Elasticity:** Quickly scale resources up or down to meet fluctuating demands, without having to invest in physical infrastructure.
- **Flexibility and Mobility:** Access data and applications from anywhere with an internet connection, on any device, promoting remote work and collaboration.
- **Increased Agility and Innovation:** Rapidly deploy new services and applications, test new ideas, and incorporate cutting-edge technologies like AI and machine learning.
- **Enhanced Security:** Reputable cloud providers invest heavily in security measures, often offering a more robust security posture than many on-premise solutions.
- **Disaster Recovery and Business Continuity:** Cloud providers offer robust backup and disaster recovery solutions, ensuring data availability and quick recovery in case of outages or disasters.
- **Automatic Updates and Maintenance:** Cloud providers handle software updates, patching, and infrastructure maintenance, freeing up internal IT teams.

Disadvantages and Concerns

- **Dependency on Internet Connectivity:** Cloud services require a stable and reliable internet connection. Outages or slow speeds can disrupt operations.
- **Security and Privacy Concerns:** While cloud providers offer strong security, concerns around data privacy, compliance, and data residency remain for some organizations.
- **Limited Control:** Users have less control over the underlying infrastructure, which can be a concern for organizations with specific customization or compliance needs.
- **Vendor Lock-in:** Migrating data and applications between different cloud providers can be complex and costly, potentially leading to vendor lock-in.
- **Cost Management Complexity:** While cost-effective, managing cloud spending can be complex due to varied pricing models and potential for unforeseen costs if not properly monitored.

- **Performance and Latency:** Depending on the location of data centers and network conditions, latency can sometimes be an issue for highly sensitive applications.

Examples of Cloud Computing in Everyday Life

Most people use cloud computing daily without realizing it:

- **Email Services:** Gmail, Outlook.com, Yahoo Mail.
- **File Storage and Sharing:** Google Drive, Dropbox, OneDrive, iCloud.
- **Streaming Services:** Netflix, Spotify, YouTube.
- **Social Media:** Facebook, Instagram, Twitter (X).
- **Online Gaming:** Cloud gaming platforms like Xbox Cloud Gaming, GeForce Now.
- **Productivity Suites:** Google Docs, Microsoft 365.

Cloud computing continues to evolve rapidly, with new services and capabilities constantly emerging, further transforming how businesses operate and how individuals interact with technology.

Case Laws:

"Case laws" refer to the body of legal principles and rules derived from judicial decisions in specific cases. In common law systems like India's, case law, also known as **precedent** or **judge-made law**, plays a fundamental role alongside statutory law (laws enacted by legislatures) and constitutional law.

The Doctrine of Precedent (Stare Decisis) in India

The Indian legal system largely follows the doctrine of stare decisis, a Latin phrase meaning "to stand by things decided." This principle mandates that courts are bound to follow the legal principles established in previous decisions by higher courts or courts of the same rank when dealing with cases with similar facts and legal issues.

Article 141 of the Constitution of India is the cornerstone of this doctrine, explicitly stating: "The law declared by the Supreme Court shall be binding on all courts within the territory of India."

Key aspects of the doctrine of precedent in India:

- **Binding Precedent:** Decisions of higher courts (e.g., Supreme Court) are absolutely binding on lower courts within their jurisdiction.
- **Persuasive Precedent:** Decisions of courts of co-ordinate jurisdiction (e.g., one High Court's decision on another High Court, or foreign judgments) are not binding but can be considered for guidance due to their persuasive value.
- **Ratio Decidendi:** Only the ratio decidendi (the essential legal reasoning or principle upon which the decision is based) of a judgment is binding.
- **Obiter Dicta:** Obiter dicta (observations or remarks made by the court that are not essential to the decision) are not binding but can have persuasive value.
- **Distinguishing Cases:** Courts can "distinguish" a previous case if the facts of the current case are materially different, thereby allowing them not to follow the precedent.
- **Overruling:** A higher court can overrule its own previous decision or a decision of a lower court if it finds the earlier decision to be incorrect or no longer relevant.
- **Per Incuriam:** A decision rendered "per incuriam" (through ignorance of a statutory provision or a binding precedent) is not considered binding.

Importance of Case Laws

Case laws are vital to the legal system for several reasons:

1. **Consistency and Predictability:** They ensure that similar cases are treated alike, promoting

fairness, certainty, and predictability in judicial outcomes. This allows individuals and businesses to better understand their legal rights and obligations.

2. **Efficiency:** Courts can rely on established legal principles, avoiding the need to re-litigate fundamental legal questions in every new case, thus saving time and resources.
3. **Guidance for Legal Professionals:** Case laws provide clarity and guidance to lawyers and judges on how laws are interpreted and applied in real-life situations.
4. **Development and Evolution of Law:** While providing stability, case laws also allow the law to evolve and adapt to changing societal norms, technological advancements, and new challenges. Judges can interpret existing laws in new contexts or even establish new legal principles when statutory law is silent or ambiguous.
5. **Checks and Balances:** Judicial interpretations through case laws act as a check on legislative and executive actions, ensuring that they conform to the Constitution and existing laws.

Landmark Case Laws in India

India has a rich history of landmark Supreme Court judgments that have significantly shaped the country's legal and constitutional landscape. Some notable examples include:

1. **Kesavananda Bharati v. State of Kerala (1973):** This is perhaps the most significant judgment in Indian constitutional history. It established the **"Basic Structure Doctrine,"** holding that while Parliament has the power to amend the Constitution, it cannot alter its "basic structure" or fundamental features (like democracy, secularism, judicial review, etc.).
2. **Maneka Gandhi v. Union of India (1978):** This case profoundly expanded the scope of **Article 21 (Right to Life and Personal Liberty)**, establishing that the "procedure established by law" must be "fair, just, and reasonable," introducing the concept of procedural due process.
3. **S.P. Gupta v. Union of India (1981) (First Judges Case), Supreme Court Advocates-on-Record Association v. Union of India (1993) (Second Judges Case), and In re Special Reference 1 of 1998 (Third Judges Case):** These cases collectively established and refined the **"Collegium System"** for the appointment and transfer of judges in higher judiciary, emphasizing the primacy of the Chief Justice of India and the collegium's opinion.
4. **Indra Sawhney & Others v. Union of India (1992) (Mandal Commission Case):** This judgment upheld the constitutional validity of 27% reservation for Other Backward Classes (OBCs) but also laid down crucial guidelines, including the "creamy layer" exclusion and the 50% reservation ceiling.
5. **S.R. Bommai v. Union of India (1994):** This ruling significantly curtailed the arbitrary use of **Article 356 (President's Rule)**, establishing that the proclamation of President's Rule is subject to judicial review.
6. **Vishaka v. State of Rajasthan (1997):** In the absence of specific legislation, the Supreme Court laid down detailed **"Vishaka Guidelines"** to prevent sexual harassment of women in the workplace, which later paved the way for the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013.
7. **Justice K.S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. (2017):** This landmark judgment unanimously declared **privacy as a fundamental right** under Article 21 of the Indian Constitution.
8. **Navtej Singh Johar v. Union of India (2018):** The Supreme Court partially decriminalized **Section**

377 of the Indian Penal Code, holding that consensual sexual acts between adults of the same gender are not criminal.

9. **Association for Democratic Reforms vs. Union of India (2024):** The Supreme Court struck down the **Electoral Bonds Scheme**, holding it unconstitutional as it violated the voters' right to information under Article 19(1)(a) of the Constitution.

These are just a few examples, and many more judgments from both the Supreme Court and various High Courts continue to shape the legal landscape in India. Studying case laws is essential for anyone involved in the legal profession or interested in understanding the nuances of the Indian legal system.

UNIT-V

Introduction To Cybercrime And Procedure To Report Cybercrime: Procedure To Report Cyber Crime, Some Basic Rules For Safe Operations Of The Computer And Internet, The Criminal Law (Amendment) Act, 2013: Legislative Remedies For Online Harassment And Cyberstalking In India

Introduction:

Cyber crime is a global threat and the evidence suggests that this threat will continue to rise. It is defined as any criminal activity which takes place on or over the medium of computers or internet other technology recognized by the information technology act. There are number of illegal activities which are committed over the internet by technically skilled criminals. Cybercrime is an uncontrollable evil having its base in the misuse of growing dependence on computers in modern life.

NATURE AND SCOPE OF CYBER CRIME:

As we all know, we live in era where most things are done over the internet, from online dealing to online transactions because the internet technology is considered a global stage.

What is Cybercrime?

Cybercrime can be defined as "The illegal usage of any communication device to commit or facilitate in committing any illegal act" or in other terms "A crime or an unlawful act where unauthorized access to some computer system without the permission of rightful owner or place of criminal activity and includes everything from online cracking to denial of service attacks.

Criminal activity is a social concept we will never be able to live in a society without cybercrime no matter how hard we try.

CHARACTERISTICS OF CYBERCRIME:

2. Cybercrimes are unlawful Act.
3. Computer is essentially an element of cyber criminality and it is either a tool or target of cybercrimes.
4. Cybercrimes are harmful Act.
5. Cybercrimes are committed in cyber space with the help of computer networking.
6. Cybercrime is a criminal activity where computer can be used to perpetuate further crime.

WHAT IS CYBERCRIME INVESTIGATION?

Cybercrime investigation is the process of identifying, analyzing, and mitigating computer based crimes and other forms of malicious activity that occur in cyberspace. It involves the use of specialized tools and techniques to investigate various types of cybercrimes, such as hacking, phishing, malware, data breaches, and identity theft.

Cybercrime investigation is a complex and constantly evolving field, as new threats and technologies

emerge. As a result, investigators must stay up-to-date with the latest techniques and tool in order to effectively investigate and mitigate cybercrimes.

TYPES OF CYBERCRIMES:

Cybercrime take many different forms, criminal who infiltrate computers and networks have developed a variety of malicious software and social engineering techniques used individually or in combination when use in in committing different types of cybercrimes. A few of the most common cybercrimes are described below.

- DDOS ATTACKS:

DDoS attacks are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

- MALWARE:

Malware or malicious software refers to any code designed to interfere with a computers normal functioning or commit a cyber crime. Common types of malware includes viruses, worms, trojans, rootkit, rogue software and various hybrid programs as well as adware, spyware, scareware and ransomware. Malware can be used to exfiltrate data, steal passwords, lock users out of their environment, destroy network resources or commandeer them to power botnets–regardless of the tactic the consequences of a successful malware attack can be severe.

- CYBER STALKING:

This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

- IDENTITY THEFT:

Identity theft occurs when someone "unlawfully obtains another individuals personal information and uses it to commit theft or fraud". Malware such as trojans and spyware are often used to steal personal information. Identity theft includes personal information such as name, Aadhar number, drivers license number, credit card number, or other identifying information.

- BOTNETS:

Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

One of the example of Botnet is Fraud Online Review, where some fake reviews are generally posted

on the device of the user.

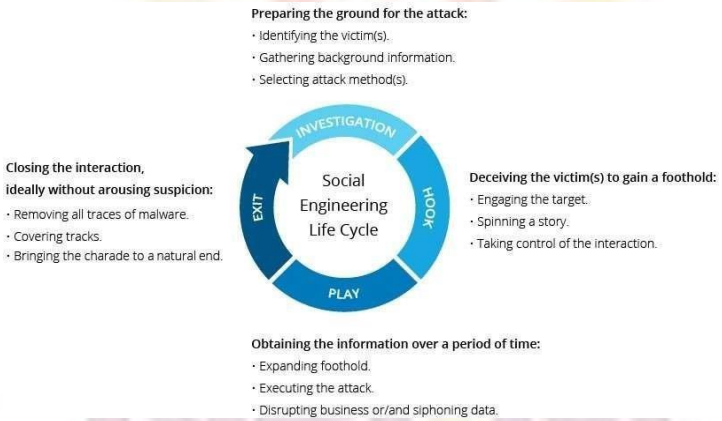
❖ SOCIAL ENGINEERING:

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. Cyber criminals use social engineering to commit fraud online.

One of the biggest weaknesses in any organization cybersecurity strategy is human error. Social engineering attacks take advantage of this vulnerability by conning unsuspecting people into compromising security and giving out sensitive information. Social engineers use various psychological hacks to trick you into trusting them or create a false sense of urgency and anxiety to lower your natural defenses.

Scammers use many different types of social engineering attacks, but some common giveaways can help you spot and avoid them.

TYPES OF SOCIAL ENGINEERING ATTACKS:



- **Phishing**: Phishing is the most common type of social engineering attack, typically using spoofed email addresses and links to trick people into providing login credentials, credit card numbers, or other personal information. Variations of phishing attacks include*:*
    - Angler phishing – using spoofed customer service accounts on social media
    - Spear phishing – phishing attacks that target specific organizations or individual
- **Whaling**:

Whaling is another common variation of phishing that specifically targets top-level business executives and the heads of government agencies. Whaling attacks usually spoof the email addresses of other high-ranking people in the company or agency and contain urgent messaging about a fake emergency or time-sensitive opportunity. Successful whaling attacks can expose a lot of confidential, sensitive information due to the high-level network access these executives and directors have.

- **Diversion Theft***:*

In an old-school diversion theft scheme, the thief persuades a delivery driver or courier to travel to the wrong location or hand off a parcel to someone other than the intended recipient. In an online diversion theft scheme, a thief steals sensitive data by tricking the victim into sending it to or sharing it with the wrong person. The thief often accomplishes this by spoofing the email address of someone in the victim's company—an auditing firm or a financial institution, for example.

- **Baiting***:*

Baiting is a type of social engineering attack that lures victims into providing sensitive information or credentials by promising something of value for free. For example, the victim receives an email that promises a free gift card if they click a link to take a survey. The link might redirect them to a spoofed Office 365 login page that captures their email address and password and sends them to a malicious actor.

- **Honey Trap*:***

In a honey trap attack, the perpetrator pretends to be romantically or sexually interested in the victim and lures them into an online relationship. The attacker then persuades the victim to reveal confidential information or pay them large sums of money.

- **Pretexting***:*

Pretexting is a fairly sophisticated type of social engineering attack in which a scammer creates a pretext or fabricated scenario—pretending to be an IRS auditor, for example—to con someone into providing sensitive personal or financial information, such as their social security number. In this type of attack, someone can also physically acquire access to your data by pretending to be a vendor, delivery driver, or contractor to gain your staff's trust.

- **SMS Phishing***:*

SMS phishing is becoming a much larger problem as more organizations embrace texting as a primary method of communication. In one method of SMS phishing, scammers send text messages that spoof multi-factor authentication requests and redirect victims to malicious web pages that collect their credentials or install malware on their phones.

Scareware:

Scareware is a form of social engineering in which a scammer inserts malicious code into a webpage that causes pop-up windows with flashing colors and alarming sounds to appear. These pop-up windows will falsely alert you to a virus that's been installed on your system. You'll be told to purchase and download their security software, and the scammers will either steal your credit card information, install real viruses on your system, or (most likely) both.

Tailgating/Piggybacking:

Tailgating, also known as piggybacking, is a social engineering tactic in which an attacker physically follows someone into a secure or restricted area. Sometimes the scammer will pretend they forgot their access card, or they'll engage someone in an animated conversation on their way into the area so their lack of authorized identification goes unnoticed.

Watering Hole:

In a watering hole attack, a hacker infects a legitimate website that their targets are known to visit. Then, when their chosen victims log into the site, the hacker either captures their credentials and uses them to breach the target's network, or they install a backdoor trojan to access the network.

CATEGORIES OF CYBER CRIME

There are three major categories of cyber crimes:

1.Crimes Against People:

These crimes include cyber harassment and stalking, distribution of child pornography, credit card fraud, human trafficking, spoofing, identity theft, and online libel or slander.

Harassment via E-Mails: This is very common type of harassment through sending letters, attachments of files & folders i.e. via e-mails. At present harassment is common as usage of social sites i.e. Facebook, Twitter, Orkut etc. increasing day by day.

Cyber-Stalking: It is expressed or implied a physical threat that creates fear through the use to computer technology such as internet, e-mail, phones, text messages, webcam, websites or videos.

Defamation: It involves any person with intent to lower down the dignity of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

Hacking: It means unauthorized control/access over computer system and act of hacking completely destroys the whole data as well as computer programs. Hackers usually hacks telecommunication and mobile network.

Cracking: It is act of breaking into your computer systems without your knowledge and consent and has tampered with precious confidential data and information.

E-Mail Spoofing: A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates.

SMS Spoofing: Spoofing is a blocking through spam which means the unwanted uninvited messages. Here a offender steals identity of another person in the form of mobile phone number and sending SMS via internet and receiver gets the SMS from the mobile phone number of the victim. It is very serious cyber crime against any individual.

Carding: It means false ATM cards i.e. Debit and Credit cards used by criminals for their monetary benefits through withdrawing money from the victim's bank account. There is always unauthorized use of ATM cards in this type of cyber crimes.

Cheating & Fraud: It means the person who is doing the act of cyber crime i.e. stealing password and

data storage has done it with having guilty mind which leads to fraud and cheating.

Child Pornography: In this cyber crime defaulters create, distribute, or access materials that sexually exploit underage children.

Assault by Threat: It refers to threatening a person with fear for their lives or lives of their families through the use of a computer network i.e. E-mail, videos or phones.

1. Crimes Against Property:

This is similar to a real-life instance of a criminal illegally possessing an individual's bank or credit card details. The hacker steals a person's bank details to gain access to funds, make purchases online or run phishing scams to get people to give away their information. They could also use a malicious software to gain access to a web page with confidential information.

Intellectual Property Crimes: Any unlawful act by which the owner is deprived completely or partially of his rights is an crime. The most common type of IPR violation may be said to be software piracy, infringement of copyright, trademark, patents, designs and service mark violation, theft of computer source code, etc.

Cyber Squatting: It involves two persons claiming for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something similar to that previously.

Cyber Vandalism: Vandalism means deliberately damaging property of another it includes destroying or damaging the data or information stored in computer when a network service is stopped or disrupted. These acts may take the form of the theft of a computer, some part of a computer.

Hacking Computer System: Hackers attacks those included Famous Twitter, blogging platform by unauthorized access/control over the computer. Those attacks were not mainly intended for financial gain too and to diminish the reputation of particular person or company. As in April, 2013 MMM India attacked by hackers.

Transmitting Virus: Viruses are programs written by programmers that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network with intent of altering or deleting it.

Cyber Trespass: It means to access someone's computer or network without the right authorization of the owner and disturb, alter, misuse, or damage data or system by using wireless internet connection.

Internet Time Thefts: Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.

2. Crimes Against Government:

When a cybercrime is committed against the government, it is considered an attack on that nation's sovereignty.

This is the least common cybercrime, but is the most serious offense. A crime against the government is also known as cyber terrorism. Government cybercrime includes hacking government websites, military websites or distributing propaganda. These criminals are usually terrorists or enemy governments of other nations.

Cyber Terrorism: Cyber terrorism is a issue in the domestic as well as global concern. Terrorist attacks on the Internet are by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer network etc. Cyber terrorism activities endanger the sovereignty and integrity of the nation.

Cyber Warfare :- It refers to politically motivated hacking to conduct sabotage and espionage.

Distribution of printed software:- It means distributed printed software from one computer to another intending to destroy the data and official records of the Government.

Possession of unauthorized information:- It is very easy to access any information by the terrorist with the aid of internet and to possess that information for political, religious, social, ideological objectives.

ACCORDING TO INDIAN CYBERCRIME COORDINATION CENTRE(I4C) CYBERCRIME CATEGORIES :

1. **CRYPTOCURRENCY CRIME**:

- **Crypto jacking:** Cryptojacking is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency.
- **Crypto Mining & Cloud Mining Scams:** Cryptocurrency-mining malware steal the resources of infected machines, significantly affecting their performance, power consumption and increasing their wear and tear.
- **Cryptocurrency Investment Frauds:** Fraudulent opportunity to invest in a cryptocurrency with guaranteed high returns e.g. "pump and dump" scams, giveaway scams, etc.

2. **CYBER TERRORISM:**

Cyber Terrorism" is committed with intent to threaten the unity, integrity, security or sovereignty

of India or to strike terror in the people or any section of the people by –

- denying or cause the denial of access to any person authorised to access computer resource; or
- attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or
- introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure.

Cyberterrorism is also committed when somebody knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

3. HACKING/DAMAGE TO COMPUTER SYSTEMS:

The act of compromising computer resources through unauthorized access to an account or computer system. It is accessing of a computer system without the express or implied permission of the owner of that computer system.

Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. Hacking / Damage to Computer Systems includes;

- Damage to computer, computer systems, etc.
- Email Hacking.
- Tampering with computer source documents.
- Unauthorised Access / Data Breach.
- Website Defacement / Hacking.

4. ONLINE AND SOCIAL MEDIA RELATED CRIME:

Online and Social media crimes in the country have been rising, posing new challenges as cyber criminals keep evolving their methods, using emerging technology. Various Cybercrimes

categorized under Online and Social Media Related Crime in the portal are as follows:

- Cheating by Impersonation
- Cyber Bullying / Stalking / Sexting
- E-Mail Phishing
- Fake/Impersonating Profile
- Impersonating Email
- Intimidating Email
- Online Job Fraud
- Online Matrimonial fraud
- Profile Hacking / Identity Theft
- Provocative Speech for unlawful acts

5. ONLINE FINANCIAL FRAUD:

Online Financial Cybercrimes include unauthorized access, sabotage, or use of computer systems with the intention to cause financial gain by cyber criminals or financial loss to the victims. It may involve computer fraud or forgery, hacking to steal personal or valuable data for commercial gain. With the increase in the use of the internet and mobile banking, online financial frauds are increasing.

Various Cybercrimes categorized under the category of Online financial fraud are as follows:

- Business Email Compromise/Email Takeover
- Debit/Credit Card Fraud/Sim Swap Fraud
- Demat/Depository Fraud
- E-Wallet Related Fraud
- Fraud Call/Vishing
- Internet Banking Related Fraud
- UPI Fraud

6. Publishing/Transmitting Of Explicit Material In Electronic Form:

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which contains sexually explicit act or conduct, or any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it shall be punished under Section 67 or 67A of IT Act.

7. RANSOMWARE:

Ransomware is a rapidly evolving form of Cybercrime, through which cyber criminals remotely

compromise and encrypt computer systems and demand a ransom in return for restoring and/or for not exposing data. Ransomware attacks target individuals and Organizations.

Ransomware attack blocks user's access to the data stored in the computer systems. More menacing versions of ransomware can encrypt files and folders on local drives, attached drives, and even networked computers.

8. CHILD PORNOGRAPHY/CHILD SEXUAL ABUSE MATERIAL(CSAM):

Child sexually abusive material (CSAM) refers to a material containing sexual image(s) in any form, of a child who is abused or sexually exploited. It is punishable to publish or transmit material depicting children in sexually explicit act or conduct in any electronic form. It is covered under **Section 67B of IT Act 2000**. Child pornography is a form of child sexual exploitation. The production, distribution, importation, reception, or possession of any image of child pornography is prohibited. Violation of child pornography/CSAM laws is a serious crime.

PROPERTY CYBER CRIME : 3rd category as mention above which includes intellectual property.

The process to report a cybercrime case in India

If you've been a victim of a cybercrime in India, it's important to report the incident to the appropriate authorities. Here are the general steps you can follow:

1. Collect All Evidences:

- **Transactions***:* Keep copies (screenshots) of any financial transactions related to the crime.
- **Screenshots***:* Capture screenshots of any relevant emails, messages, or online conversations.
- **Passwords***:* Change your passwords for all affected accounts immediately in case of social media-related cybercrimes.

2. Identify the Appropriate Authority:

- *Call 1930:* The National Helpline number for reporting financial cyber frauds in India is 1930.
- *Cyber Crime Reporting Portal:* Visit the National Cybercrime Reporting Portal (https://cybercrime.gov.in/) and file a complaint online.
- *Local Police Station:* If the crime is serious or urgent, report it to your local police station immediately.

How to file a cybercrime complaint online?

Step 1*:* Visit the National Cybercrime Reporting Portal https://cybercrime.gov.in

Step 2*:* Click on the Register a Complaint

Step 3*:* Select the cybercrime category

Option 1 – Women/Children Related Crime

Option 2 – Financial Fraud

Option 3 – Other Cybercrimes

Step 4*:* Click on the relevant category option and "Register a Complaint"

Step 5*:* Click on File a Complaint

Step 6*:* Click on I Accept

Step 7*:* Click here for new user

Step 8*:* File details and verify the account

Step 9*:* Fill in all the details related to cybercrime

- **Provide Details***:* Clearly explain the nature of the crime, including dates, times, and any financial losses.
- **Submit Evidence***:* Attach the collected evidence to your complaint.

Some basic rules for safe operations of the computer and internet:

It's excellent that you're asking about basic rules for safe computer and internet operations! In today's digital world, cybersecurity is paramount, and following fundamental practices can prevent many common issues. Here are some essential rules for safe computer and internet usage:

I. General Computer Safety Rules:

1. Keep Your Software Updated:
    - Operating System (OS): Enable automatic updates for your OS (Windows, macOS, Linux). These updates often include critical security patches that fix vulnerabilities.
    - Applications: Regularly update all your software, including web browsers, antivirus programs, office suites, and any other applications you use. Outdated software is a common entry point for malware.
2. Use Strong, Unique Passwords:
    - Complexity: Use a combination of uppercase and lowercase letters, numbers, and symbols.
    - Length: Aim for at least 12-16 characters. Longer is generally better.
    - Uniqueness: Never reuse passwords across different accounts. If one account is compromised, others remain safe.
    - Password Manager: Consider using a reputable password manager (e.g., LastPass, Bitwarden, 1Password) to generate, store, and manage complex passwords securely.
3. Enable Multi-Factor Authentication (MFA/2FA):
    - Wherever possible (email, banking, social media, shopping sites), enable MFA. This adds an extra layer of security, typically requiring a code from your phone, a fingerprint, or a hardware key in addition to your password. Even if your password is stolen, the attacker can't access your account without the second factor.
4. **Use Reputable Antivirus/Anti-Malware Software:**
    - Install and keep an updated antivirus program on your computer.
    - Run regular scans to detect and remove threats.
    - Many operating systems (like Windows Defender) have built-in solutions that are quite effective when kept updated.
5. **Back Up Your Data Regularly:**
    - Crucial for protecting against data loss from hardware failure, malware (especially ransomware), or accidental deletion.
    - Use external hard drives, cloud storage services (e.g., Google Drive, OneDrive, Dropbox), or a combination.
    - Test your backups periodically to ensure they are recoverable.
6. **Be Wary of Removable Media:**
    - Avoid inserting unknown USB drives, external hard drives, or CDs/DVDs into your computer.

They can carry malware.

- Scan any removable media with antivirus software before opening files from it, even if you know the source.

7. **Limit Account Privileges:**
    - Use a standard user account for daily activities and only switch to an administrator account when necessary for installing software or making system changes. This limits the damage malware can do.
8. **Physical Security:**
    - Don't leave your computer unattended in public places.
    - Use screen locks and password protection.
    - Consider using a Kensington lock or similar physical security device for laptops.

II. Internet Safety Rules:

1. **Be Skeptical of Emails and Messages (Phishing/Smishing/Vishing):**

- Don't click on suspicious links: Especially from unknown senders or emails that seem "too good to be true."
- Verify the sender: Even if it looks like a legitimate sender (bank, government, popular service), check the sender's actual email address. It often won't match the displayed name.
- Beware of attachments: Don't open unexpected attachments, particularly those with unusual file extensions (e.g., .exe, .zip, .js) unless you are absolutely sure of their legitimacy.
- Look for red flags: Poor grammar, urgent or threatening language, requests for personal information, and generic greetings.
- If in doubt, go directly to the source: If an email purports to be from your bank, don't click the link. Instead, type your bank's official URL directly into your browser or use their official app.

2. **Browse Securely (HTTPS):**

- Always look for "https://" at the beginning of a website's URL and a padlock icon in your browser's address bar. This indicates that your connection to the website is encrypted, protecting your data in transit.
- Avoid entering sensitive information (passwords, credit card details) on websites that do not use HTTPS.

3. **Use a Virtual Private Network (VPN) on Public Wi-Fi:**

- Public Wi-Fi networks (cafes, airports) are often insecure and vulnerable to eavesdropping.
- A VPN encrypts your internet traffic, protecting your data from potential attackers on the same

network.

4. **Be Mindful of What You Share Online:**

- Personal Information: Be cautious about sharing personal details like your full birth date, home address, phone number, financial information, or daily routines on social media or public forums. This information can be used for identity theft or targeted attacks.
- Photos/Videos: Think twice before posting images that reveal too much personal information or could be used to compromise your privacy or safety.
- Location Services: Be selective about enabling location services on apps and social media, as this can reveal your whereabouts.

5. **Manage Your Privacy Settings:**
    - Regularly review and adjust the privacy settings on your social media accounts, email, and other online services. Control who can see your posts, information, and contact you.
6. **Be Cautious with Downloads:**

- Only download software, apps, and files from official and trusted sources (e.g., official app stores, publisher websites).
- Be very careful with free software or content from unofficial sites, as they often bundle malware.

7. **Think Before You Click (Even on Social Media):**

- Clickbait links, quizzes, or enticing offers on social media can lead to malware or phishing sites. If it seems too good to be true, it probably is.

8. **Be Aware of Social Engineering:**

Attackers often try to manipulate you into divulging information or taking actions against your interest. They might impersonate someone you trust or create a sense of urgency. Always verify requests for sensitive information.

By consistently applying these basic rules, you can significantly reduce your risk of falling victim to cyber threats and enjoy a safer computing and internet experience.

Some basic rules for safe operations of the computer and internet:

It's great you're looking for basic rules for safe computer and internet operations! In today's digital world, adhering to fundamental security practices is crucial to protect yourself and your data.

Here are some essential rules, categorized for clarity**:**

I. General Computer Safety Rules

1. **Keep Your Software Up-to-Date:**

- Operating System (OS): Always enable automatic updates for your computer's operating system

(Windows, macOS, Linux). These updates often contain critical security patches that fix vulnerabilities exploited by attackers.

- Applications: Regularly update all other software, including web browsers, antivirus programs, office suites, and any other applications you use frequently. Outdated software is a common weak point for malware.

2. **Use Strong, Unique Passwords for Every Account:**

- Complexity: Create passwords that are a mix of uppercase letters, lowercase letters, numbers, and symbols.
- Length: Aim for passwords that are at least 12-16 characters long. Longer passwords are significantly harder to crack.
- Uniqueness: Never reuse passwords across different accounts. If one service is breached, all your other accounts using the same password could be compromised.
- Password Manager: Consider using a reputable password manager (e.g., LastPass, Bitwarden, 1Password) to securely generate, store, and manage your complex, unique passwords.

3. **Enable Multi-Factor Authentication (MFA/2FA) Whenever Possible:**

- This adds an extra layer of security beyond just a password. After entering your password, you'll need to provide another piece of verification, such as a code sent to your phone, a fingerprint scan, or a response from an authenticator app. Even if your password is stolen, attackers can't get in without the second factor.

4. **Install and Maintain Reputable Antivirus/Anti-Malware Software:**

- Have a good antivirus program installed on your computer and ensure it's always up to date.
- Run regular, full system scans to detect and remove any malicious software that might have slipped through.
- Many operating systems (like Windows with its built-in Windows Defender) offer effective solutions when kept current.

5. **Back Up Your Important Data Regularly:**

- This is your best defense against data loss due to hardware failure, accidental deletion, or cyberattacks like ransomware.
- Use external hard drives, cloud storage services (e.g., Google Drive, Microsoft OneDrive, Dropbox), or a combination of both.
- Periodically test your backups to ensure they can be restored successfully.

6. **Be Cautious with Removable Media:**

- Never insert unknown USB drives, external hard drives, or CDs/DVDs into your computer. They can easily carry malware.
- If you must use a removable device, scan it with your antivirus software before opening any files.

7. Limit User Account Privileges:

- For daily computing, use a standard user account instead of an administrator account. Only switch to an administrator account when you need to install software or make system-level changes. This limits the potential damage malware can do.

8. Ensure Physical Security of Your Device:

- Don't leave your computer or mobile devices unattended in public places.
- Always use a password or PIN to lock your screen.
- For laptops, consider using a physical security cable lock if you're in a shared environment.

II. Internet Safety Rules

1. Be Highly Skeptical of Emails, Messages, and Calls (Phishing/Smishing/Vishing):

- Do not click on suspicious links: Especially from unknown senders or if the email seems "too good to be true" or creates a sense of extreme urgency/threat.
- Verify the sender: Even if an email *looks* like it's from a legitimate company (your bank, utility provider, a well-known service), check the actual sender's email address. Often, it won't match the displayed name.
- Beware of unexpected attachments: Never open attachments, especially those with unusual file extensions (.exe, .zip, .js, .scr), unless you are absolutely certain of their source and purpose.
- Look for red flags: Poor grammar, generic greetings ("Dear Customer"), urgent demands for personal information, or threats of account suspension.
- If in doubt, go directly to the source: If an email purports to be from your bank, don't click the link. Instead, open your browser and type your bank's official website address directly, or use their official app.

2. Always Look for "HTTPS" and the Padlock Icon:

- When Browse, especially on websites where you enter personal or financial information, ensure the URL starts with https:// and there's a padlock icon in your browser's address bar. This indicates a secure, encrypted connection, meaning your data is protected during transmission. Avoid entering sensitive info on sites that only show http://.

3. Use a Virtual Private Network (VPN) on Public Wi-Fi:

- Public Wi-Fi networks (cafes, airports, hotels) are often unsecured and can be easily intercepted by malicious actors. A VPN encrypts your entire internet connection, protecting your data from eavesdropping when you're on public networks.

4. **Be Mindful of What You Share Online:**

- Personal Information: Be extremely cautious about sharing sensitive personal details (full birth date, home address, phone number, financial info, specific travel plans, daily routines) on social media or public forums. This information can be used for identity theft or targeted attacks.
- Photos/Videos: Think before you post images that reveal too much personal information or could compromise your privacy or the privacy of others.
- Location Services: Be selective about enabling location services on apps and social media, as this can inadvertently reveal your whereabouts.

5. **Review and Adjust Your Privacy Settings:**

- Regularly check and configure the privacy settings on all your social media accounts, email providers, and other online services. Control who can see your posts, information, and how you are contacted.

6. **Download from Official and Trusted Sources Only:**

- Only download software, apps, and files from official app stores (e.g., Google Play Store, Apple App Store), reputable publisher websites, or well-known and trusted sources. Avoid third-party download sites or pirated content, as they often bundle malware.

7. **Think Before You Click (Even on Social Media):**

- Be wary of sensational clickbait, "too good to be true" offers, or suspicious quizzes/games on social media. These often lead to phishing sites, malware downloads**,** or scams.

8. **Understand and Be Aware of Social Engineering:**

- Cybercriminals often use psychological manipulation (social engineering) to trick you into revealing information or performing actions. They might impersonate someone you trust, create a false sense of urgency, or appeal to your curiosity. Always pause and verify before acting on unusual requests**.**

Criminal LAW

- The Criminal Law (Amendment) Act, 2013, was enacted for growing concerns over crimes against women, particularly in the aftermath of the 2012 Delhi gang-rape incident. This legislation brought significant reforms to the Indian Penal Code, 1860 (IPC), the Code of Criminal Procedure, 1973 (CrPC), the Indian Evidence Act, 1872 (IEA), and the Protection of Children from Sexual Offences Act, 2015 (POCSO). The amendments aimed to enhance the legal framework to ensure stricter

punishment for sexual offences and provide better protection and justice for victims.

When was the Criminal Law (Amendment) Act, 2013 Enacted and Enforced?

The Criminal Law (Amendment) Act, 2013, passed by Parliament and receiving Presidential assent on 2nd April 2013, came into force retrospectively from 3rd February 2013. It introduced several new offences and redefined existing provisions to broaden their scope. Important amendments include provisions related to acid attacks, sexual harassment, voyeurism, stalking, and human trafficking.

Sections 354A to 354D IPC:

Section 354A: It was inserted to introduce punishments for sexual harassment, including unwelcome advances, demands for sexual favors, and showing pornography.

Section 354B: It was inserted to penalize assault with intent to disrobe a woman.

Section 354C: It was inserted to criminalize voyeurism, with enhanced penalties for repeat offenders.

Section 354D: It was inserted to punish stalking, including online harassment.

Cyber stalking is a type of a crime. In the cyber stalking there is a involvement of two persons- **Firstly**, the stalker is also known as attacker who do the crime & Secondly, the Victim who is harassed by that stalker.

Cyber stalking is also known as cyber crime. Cyber which is related to the internet and the stalking means to browsing anyoneâ online history with the help of any social media or in other websites to know about that particular person is term as stalking.

2. Stalking

The only term stalking means to consistently following any particular person over a long period of time. This activity also involves the harassment or threatening behavior. The

stalker consistently following a person everywhere at home, market etc, and the stalker also threaten that person by repeatedly sending the messages, doing blank phone calls. but, in the cyber stalking there is a use of the internet or any other electronic media by which the communication can be done through the E-mails or SMS to stalk that person. A cyber stalkerâ€™s totally relies upon the inconspicuousness given by the internet, which allows them to stalk their victim without being detected. The cyber stalking is totally different from the spamming of the messages by the spammer. Cyber stalking is a serious crime and there are many cases against it in India.

3. How the Case of Cyber Stalking are dealth within the Indian Laws?

Cyber stalking is a serious crime, a type of offence committed by the personâ€™s known as the stalkers. There are many cases filed against those persons by the victim every year in India.

In India the cases which are filed against those stalkers are majorly reported by the females, nearly about 60% females get victimized. The stalking is majorly spotted in the two states of India;

Firstly, Maharashtra with 1,399 cases which had a higher number of stalking. Secondly, Delhi with around 1130 cases is filed against the stalking.

The cyber stalking cases are dealt in India by the:

1. Information technology act 2000.
2. The criminal law (Amendment) act 2013.

1. Information Technology Act 2000

If any person is publishing or sending any salacious material in the form of electronic media is to be charged under section 67 of the Act. This dose not involves the determination of the extent of liability of ISP (internet service providers) and their directors.

For the preclusion of cyber stalking the protection of the data is very important, which gets leaked easily by the hackers. According to the amended IT act, section 43 A is added for the inclusion of a Body corporateâ€• , the allowing of the compensation in the case of a firm or a company which causes any wrongful losses or gain to any person by the way of transmitting any sensitive

information and the maintenance of such type of security, then such body corporate shall be liable to pay damages by way of compensation.

The Information Technology Act, 2000 also comes into picture when the cyberstalker posts or sends any obscene content to the victim. Section 67 of the Information Technology Act states that when any obscene material is published, transmitted or caused to be published in any electronic form, then it is a crime of obscenity, punishable with imprisonment for up to 5 years with fine of up to Rs. 1 lakh. A second or subsequent conviction is punishable by imprisonment for up to 10 years with a fine of up to Rs. 2 lakh.

Section 500 of the Indian Penal Code that deals with defamation, can be applied in case of cyber stalking in India if the stalker forges the victimâ€™s personal information to post an obscene message or comment on any electronic media. Section 500 criminalises publishing any false statement against a person or harming the person's reputation and provides punishment for any such act with imprisonment up to 2 years, fine or both.

The first ever complaint against cyber stalking in India was filed by Ritu Kohli in 2003, whose name and contact information was posted by her husbandâ€™s friend on a chatting site, without her permission. She filed a complaint with the cyber cell in India under Section 509 of the Indian Penal Code for outraging her modesty.

The crime of cyber stalking in India is prominently increasing, with new cases of internet stalking every day. With ease in accessing personal information of a person online, cybercriminals are easily able to stalk and harass a person.

The criminal law (Amendment) Act, 2013

This act states that, Any man who

I. contacts and follows a woman or attempts to contacts such woman to proselytize personal communication repeatedly despite of being clear indication of disinterest by such woman or;

II. Observe the use of a woman over the internet, instant messages, e-mail or any other form of electronic communication in cyber stalking.

- The Virtual Reality of Cyber Stalking in India
- The internet has created a channel that has made communication and sharing of data easier. Social media platforms allow people to connect with each other and access each other's

information with a single click. However, on the flip side, technology has certain loopholes which allow criminals to misuse this liberty of access, leading to a rise in cyber crimes.

- The internet has created a channel that has made communication and sharing of data easier. Social media platforms allow people to connect with each other and access each otherâ€™s information with a single click.
- However, on the flip side, technology has certain loopholes which allow criminals to misuse this liberty of access, leading to a rise in cyber crimes.Section 66A of the Information Technology Act, 2000 states that a person would be punished with imprisonment for up to 3 years with fine if he uses a computer resource or communication device to send Any information that is grossly offensive or has menacing character.
- Any information which is false to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will
- Any email or electronic mail message to cause annoyance or inconvenience, mislead the addressee or recipient about the origin of such messages.

Legislative Remedies For Online Harassment And Cyberstalking In India:

Online harassment and cyberstalking are serious concerns in India, given the rapid growth of internet penetration. While India doesn't have a single, dedicated law specifically termed "Cyberbullying Law," the existing legal framework draws primarily from the **Information Technology Act, 2000 (IT Act)** and the **Indian Penal Code, 1860 (IPC)**, along with other specialized laws like the **Protection of Children from Sexual Offences (POCSO) Act, 2012**, to address these offenses.

Here's a breakdown of the key legislative remedies:

Information Technology Act, 2000 (IT Act) and its Amendments

The IT Act is the primary law in India dealing with cybercrimes and electronic commerce. Several sections are invoked for online harassment and cyberstalking:

1. **Section 66E - Punishment for violation of privacy:**
    - This section penalizes the unauthorized capture, publication, or transmission of images of a private area of any person without their consent, under circumstances where the person would have a reasonable expectation of privacy.
    - **Penalty:** Imprisonment up to three years or a fine up to two lakh rupees (INR 200,000), or both.
    - **Section 67 - Punishment for publishing or transmitting obscene material in electronic form:**

- Criminalizes the publication or transmission of any material in electronic form that is "lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it."
- **Relevance:** Applicable when online harassment involves sending or posting sexually explicit or vulgar content.
- **Penalty:** Imprisonment up to three years and a fine up to five lakh rupees (INR 500,000) for the first conviction. For subsequent convictions, it extends to imprisonment up to five years and a fine up to ten lakh rupees (INR 1,000,000).
- **Section 67A - Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form:**
- Specifically deals with content depicting sexually explicit acts.
- **Relevance:** Used for more severe forms of explicit content sharing as part of harassment.
- **Penalty:** Imprisonment up to five years and a fine up to ten lakh rupees (INR 1,000,000) for the first conviction. For subsequent convictions, it can extend to imprisonment up to seven years and a fine up to ten lakh rupees.
- **Section 67B - Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form:**
- This section specifically targets child pornography and any related content.
- **Relevance:** Crucial for prosecuting severe offenses involving minors in cyber harassment.
- **Penalty:** Very stringent penalties, including imprisonment up to five years and a fine up to ten lakh rupees for the first conviction, with increasing penalties for subsequent offenses.
- **Section 66C - Punishment for identity theft:**
- Addresses the fraudulent or dishonest use of electronic signatures, passwords, or any other unique identification feature of another person.
- **Relevance:** Relevant when cyberstalkers create fake profiles, impersonate victims online, or gain unauthorized access to their accounts.
- **Penalty:** Imprisonment up to three years and a fine up to one lakh rupees (INR 100,000).
- **Section 66D - Punishment for cheating by personation by using computer resource:**
- Deals with cheating by impersonating another person using a computer resource or communication device.
- **Relevance:** Similar to 66C, but specifically applicable if the impersonation is for the purpose

of cheating or defrauding.

- **Penalty:** Imprisonment up to three years and a fine up to one lakh rupees.
- **Section 43A - Compensation for failure to protect data:**
- While not a criminal remedy for harassment itself, this section holds a body corporate liable to pay compensation if it is negligent in implementing and maintaining reasonable security practices and procedures for sensitive personal data, leading to wrongful loss or gain.
- **Relevance:** Important in cases where a data breach facilitated or contributed to online harassment.
- **II. Indian Penal Code, 1860 (IPC)**
- Several sections of the IPC are frequently invoked for online harassment and cyberstalking, often alongside the IT Act, due to the overlap with traditional crimes:
- **Section 354D - Stalking:**
- This is the most direct provision addressing stalking, specifically including its online form. It penalizes any man who:
- Follows a woman and contacts, or attempts to contact, such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman; or
- Monitors the use by a woman of the internet, email, or any other form of electronic communication.
- **Exceptions:** Lawful and for official duty, or pursuing in discharge of a legal duty, or under any law, or any conduct which is reasonable and in the particular circumstances.
- **Penalty:** Imprisonment up to three years and/or a fine for the first conviction. For a second or subsequent conviction, imprisonment up to five years and/or a fine. (Note: The first offense is bailable, but subsequent offenses are non-bailable).
- **Section 509 - Word, gesture or act intended to insult the modesty of a woman:**
- Applies to any person who, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen by such woman, or intrudes upon the privacy of such woman.
- **Relevance:** Covers many forms of online verbal, textual, or visual harassment that insult a woman's modesty.
- **Penalty:** Imprisonment up to three years and/or a fine.
- **Section 499 (Defamation) & Section 500 (Punishment for defamation):**

- If online harassment involves posting false or damaging statements about a person that harm their reputation, these sections apply. Online defamation is a significant issue.
- **Penalty:** Simple imprisonment up to two years, or with fine, or both.
- **Section 503 (Criminal Intimidation) & Section 506 (Punishment for criminal intimidation):**
- If the online harassment involves threatening someone with injury to their person, reputation, or property, these sections can be invoked.
- **Relevance:** Applicable for threats received via messages, emails, or social media.
- **Penalty:** Imprisonment up to two years, or with fine, or both. If the threat is to cause death, grievous hurt, or destruction of property by fire, etc., or to impute unchastity to a woman, the punishment can be higher.
- **Section 507 - Criminal intimidation by an anonymous communication:**
- Specifically deals with criminal intimidation if done through anonymous communication, which is very common in online harassment scenarios.
- **Relevance:** Addresses threats where the perpetrator's identity is concealed.
- **Penalty:** Adds to the punishment under Section 506, extending imprisonment for a term that may extend to two years.
- **Section 354A - Sexual Harassment and Punishment for Sexual Harassment:**
- While often associated with physical acts, online components that constitute "sexual harassment" (e.g., sexually colored remarks sent repeatedly, demands or requests for sexual favors through electronic means) can also be covered.
- **III. Protection of Children from Sexual Offences (POCSO) Act, 2012**
- This is a crucial special law for protecting children from sexual abuse and exploitation. If online harassment or cyberstalking involves a minor (under 18 years of age), the POCSO Act will apply, ensuring more stringent penalties and a child-friendly judicial process.
- **Sections 13-15:** Deal with using children for pornographic purposes, including publishing, transmitting, or storing child pornography.
- **Other sections:** Can be invoked if online acts lead to or facilitate other sexual offenses against children.
- **IV. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**
- These rules are vital for addressing online harm, as they place significant obligations on

social media platforms, internet service providers, and other intermediaries:

- **Due Diligence:** Mandate that intermediaries exercise due diligence to prevent the hosting or sharing of unlawful content.
- **Removal of Content:** Require intermediaries to remove or disable access to unlawful content (including harassment, explicit material, impersonation, etc.) within specific timeframes upon receiving a court order, government notification, or a user complaint (especially for sexually explicit content, which requires removal within 24 hours of receiving a complaint).
- **Grievance Redressal:** Require intermediaries to establish a grievance redressal mechanism, including a Grievance Officer, to address user complaints.
- **Traceability of Originator (for Significant Social Media Intermediaries):** For certain serious offenses (like those under Sections 354A, 354B, 354C, 354D, 507, 509 of the IPC, or Section 66E of the IT Act), significant social media intermediaries providing messaging services must enable the identification of the first originator of the information, if required by a court order or a competent authority. This is a contentious provision but aims to tackle the anonymity challenge.
- **V. Reporting Mechanisms**
- **National Cybercrime Reporting Portal (cybercrime.gov.in):** Launched by the Ministry of Home Affairs, this online portal allows victims to report various cybercrimes, including online harassment, cyberstalking, and child sexual abuse material (CSAM). Complaints are then routed to the relevant state/UT law enforcement agencies.
- **Direct Approach to Law Enforcement:** Victims can also file a First Information Report (FIR) directly at a local police station or a dedicated Cyber Cell.
- **Challenges and Future Directions**
- Despite this framework, challenges persist:
- **Jurisdictional Issues:** The borderless nature of the internet makes it difficult to prosecute offenders located in other countries.
- **Anonymity & Attribution:** The ease of creating fake profiles and using VPNs makes it challenging to identify and track perpetrators.
- **Evidence Collection & Preservation:** Digital evidence is ephemeral and requires specialized skills for collection, preservation, and presentation in court.
- **Lack of Public Awareness:** Many victims are still unaware of the existing laws and

reporting mechanisms.

- **Digital Literacy:** A lack of digital literacy among both victims and, in some cases, law enforcement, can hinder effective response.
- **Evolving Nature of Cybercrime:** Cybercriminals constantly adapt, requiring continuous updates to laws and enforcement strategies.
- **Enforcement Effectiveness:** The speed and efficacy of police investigations and judicial processes can vary.
- The Indian government and judiciary are increasingly focused on cyber safety. There is an ongoing discourse about potentially introducing more comprehensive legislation specifically tailored to online safety and digital harms, but currently, the remedies largely rely on the existing, though robust, combination of the IT Act and IPC. Continuous awareness campaigns, capacity building for law enforcement, and international cooperation remain crucial for effective deterrence and redressal of online harassment and cyberstalking.