



# PMCA605L : Cyber Security

**Module 5: Cybercrimes and Cyber Security - The Legal Perspectives**

Courtesy: Nina Godbole, Sunit Belapure *& Other Sources of Internet*

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Dr. R. K. Nadesh

# The Legal Perspectives

As per the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders.

**1. Cybercrime in a restrictive sense (computer crime):** Any illegal behavior carried out by means of electronic methods targeting the security of computer systems and the data processed by them.

**2. Cybercrime in a general sense (computer-related crime):** Any illegal behavior committed by means of, or in relation to, a computer system or network.

***Crime or an offense is "a legal wrong that can be followed by criminal proceedings which may result into punishment."***

# Examples

- Unauthorized access to computer
- Causing damage to computer or data or program
- An act of computer sabotage
- Doing unauthorized interception of communications
- Carrying out Computer Espionage.

## Unauthorized access to computer

- **Section18.2 -152.4 of Virginia State Criminal Law**

✓ Temporarily or Permanently remove computer data or program or software from a computer or computer network.

✓ Cause a computer to malfunction

✓ Alter or Erase a computer data or program or software

✓ Effect the creation or alteration of a financial instrument or of an electronic transfer of funds.

# Special Crimes Under Cyber Crimes in IPC (Indian Penal Code)

- India addresses cyber crimes under **both the IPC (Indian Penal Code) and the IT Act, 2000**

- Below are some **special cyber crimes** covered under the **IPC**:

## Identity Theft & Cheating by Personation (Online Fraud)

- IPC Section 419 – Punishment for cheating by impersonation (up to 3 years imprisonment or fine, or both).
- IPC Section 420 – Punishment for cheating and dishonestly inducing delivery of property (up to 7 years imprisonment and fine).

Example: Fake online profiles used for scams, phishing attacks, or financial fraud.

## Cyber Crimes in IPC (Indian Penal Code)

- **IPC Section 354D** – Stalking, including online stalking (punishment: 3 years for first offense, 5 years for repeat offense).

- **IPC Section 499 & 500** - Criminal defamation for harming someone's reputation online (punishable by imprisonment up to 2 years and a fine).

- **IPC Section 441 & 447** – Unauthorized access to a computer system or network.

- **IPC Section 378 & 424** – Theft and misappropriation of data or digital property.

# Cybercrime Law Scenario (Asia-Pacific Region)

## ***Challenges***

- The general lack of awareness of information security issues.
- The rapidly evolving complexity, capacity and reach of ICT.
- The anonymity afforded by these technologies and the transnational nature of communication networks.

# Data protection laws

- Data protection laws permit and even facilitate the use of personal data while providing to individuals:

➢control over what to disclose

➢awareness of how their personal data will be used

➢rights to insist that data are accurate and up to date, and protection when personal information is used to make decisions about a person.

# Online Safety and Cybercrime Laws

***Numerous regional norms:***

- *A*sia-*P*acific *E*conomic *C*o-operation (APEC) Privacy Framework
- EU's Data Protection Directive
- Council of Europe's (CoE) on Cybercrime

# Data Privacy and Data Protection

- The Microsoft-drafted Model Privacy Bill (the Model Bill) serves as a benchmark legislation in the data privacy arena.

- It aligns with the Fair Information Practice Principles (FIPS) and emphasizes that privacy-mature organizations must provide a privacy notice before collecting personally identifiable information (PII).

# Privacy Notice

- Privacy notice is crucial because it ensures legal compliance and entitles an organization to use or disclose personal data for secondary purposes (e.g., marketing, analytics) only with informed consent.

✓ What **personal data** is collected?
How the data will be **used and stored?**
Whether it will be **shared or sold** to third parties?
What **rights** do individuals have over their data?

# From privacy perspective

- Two Key Types of Information (From a Privacy Perspective)

## Aggregated Information

- Data that is **compiled and anonymized** so it cannot be linked to an individual.
  Used for analytics, research, and trend identification.
  **Example:** "40% of users visit our website via mobile devices.“

## Personally Identifiable Information (PII)

- **Data that can directly or indirectly identify a person.**
  Can be sensitive (financial, health records) or non-sensitive (email, name, IP address).
  Example: Name, phone number, social security number, biometric data, etc.

# Global Data Privacy Laws

- **GDPR (EU)** – Strongest privacy regulations; requires explicit user consent. (**General Data Protection Regulation** )

- **CCPA (California, U.S.)** – Gives users the right to know, delete, and opt out. (**California Consumer Privacy Act**)

- **DPDP Act (India, 2023)** – Focuses on consent, data localization, and user rights. (**Digital Personal Data Protection**)

# Spam Laws

***The Microsoft checklist features effective anti-spam legislation and is considered as the benchmark legislation:***

- Envisages an “Opt-Out” anti-spam regime to address commercial electronic messages.
- Mentions that transactional or relationship messages to customers should be excluded from the scope of regulation.
- It contains the usual restrictions on transmitting electronic messages of a commercial nature.
- Mentions that customers should be able to opt out from the receipt of commercial electronic messages on a product line.
- It does not contemplate any “ADV” or other labeling requirement.

# Summary

- **Opt-Out Mechanism** – The legislation supports an "Opt-Out" system, meaning recipients must be given a clear way to unsubscribe from commercial electronic messages.

- **Exclusions for Transactional Messages** – Messages related to transactions or customer relationships (e.g., order confirmations, account updates) are not covered under spam regulations.

- **Restrictions on Commercial Messages** – Standard restrictions apply to electronic messages of a commercial nature, likely including prohibitions on deceptive practices.

- **Product-Line Opt-Out** – Customers should be able to unsubscribe from commercial messages specific to a product line, rather than all communications from a company.

- **No Labeling Requirement** – The checklist does not mandate using labels like “ADV” (Advertisement) in subject lines or message content.

# Is Spam Harmful?

- Content (Harmful Embedded Code)
- Internet Resources Consumed (Bandwidth, Storage, Memory & Other resources)
- Threat to Internet Security (Company's Reputation)
- Privacy Violations
- Financial Losses
- Network Congestion & System Overload

# Anti-Spam Legislation

- **Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018- Telecom Regulatory Authority of India (TRAI)**.

- These regulations aim to combat **Unsolicited Commercial Communication (UCC)** through SMS and calls but do not specifically address email spam. (**Do Not Disturb (DND) Registry**)

- **Email Spam Not Covered** – Unlike the U.S. **CAN-SPAM Act** or **GDPR (EU),** India's rules focus only on mobile communication, leaving email spam largely unregulated.

# Online Protection for Children

COPPA (Children's Online Privacy Protection Act)

COPPA is a U.S. federal law designed to protect the privacy of children under 13 years of age by regulating the online collection of their personal information.

Key Provisions:

**Parental Consent:** Websites and online services must obtain verifiable parental consent before collecting, using, or disclosing personal information from children.

**Transparency:** Operators must post a clear privacy policy detailing their information practices concerning children.

**Data Limitations:** The law restricts the amount and type of data that can be collected from children, thereby reducing potential risks from data breaches and misuse.

# Why Do We Need Cyber laws: The Indian Context

- Intellectual property
- Data protection and privacy
- Freedom of expression
- Crimes committed using computers

The Indian Parliament passed its first cyberlaw (ITA 2000) -- aimed at providing the legal infrastructure for E-Commerce in India.

# Information Technology Act, 2000 (ITA 2000)

- Based on Model UNCITRAL (United Nations Commission On International Trade Law) law for E-Commerce
- The law of the land in India
- Manages all aspects, issues, legal consequences, and conflict in the world of cyberspace, the Internet or WWW

- It provides the statutory backbone for conducting e-commerce, securing digital communications, and establishing legal validity for electronic records and signatures.
- The **Information Technology Act, 2000 (IT Act)** is the primary legislation in India governing cyber activities, digital transactions, and cybersecurity.
- It provides legal recognition to electronic transactions, aims to prevent cybercrimes, and establishes penalties for cyber-related offenses.

# The Indian IT Act, ITA 2000

## 1. Legal Recognition of Electronic Transactions

- Recognizes electronic documents, digital signatures, and online contracts as legally valid.
- Facilitates e-commerce and digital transactions.

## 2. Cybercrimes and Penalties

- Defines and penalizes cyber offenses such as hacking, identity theft, phishing, and cyber-terrorism.
- Punishments range from fines to imprisonment, depending on the severity of the crime.

# The Indian IT Act, ITA 2000

## 3. Data Protection and Privacy

- Section 43A mandates compensation for failure to protect personal data.
- Section 72 penalizes unauthorized disclosure of personal information.

## 4. Regulation of Certifying Authorities

- Establishes a framework for issuing Digital Signatures and regulates Certifying Authorities (CAs).

# The Indian IT Act, ITA 2000

**5. Establishment of the Cyber Appellate Tribunal**

- Provides a mechanism for handling disputes related to cybercrimes and electronic transactions.

**Admissibility of Electronic Records: Amendments made in the Indian ITA 2000**

- Amendment of three acts (as per the Second, Third and Fourth Schedule of the Indian ITA 2000):
- The Indian Evidence Act 1872
- The Bankers' Books Evidence Act 1891
- The Reserve Bank of India Act 1934

# IT Act and its provisions

| Chapter | Coverage |
|---|---|
| Chapter I: Preliminary | • Act extends to the whole of India (Section 1)<br>• Exceptions to Applicability (Section 1(4)) |
| Chapter II: Digital Signature | • Authentication of electronic records (Section 3)<br>• Legal Framework for affixing Digital signature by use of asymmetric crypto system and hash function (Section 3) |
| Chapter III: Electronic Governance | • Legal recognition of electronic records (Section 4)<br>• Legal recognition of digital signatures (Section 5)<br>• Retention of electronic record (Section 7)<br>• Publication of Official Gazette in electronic form (Section 8) |

# IT Act and its provisions

| Chapter | Coverage |
|---|---|
| Chapter IV | • Attribution, Acknowledgement and Receipt of Electronic Documents |
| Chapter V | • Security procedure for electronic records and digital signature (Sections 14, 15, 16) |
| Chapter VI - VIII | • Licensing and Regulation of Certifying authorities for issuing digital signature certificates (Sections 17-34)<br>• Functions of Controller (Section 18)<br>• Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities (Section 19)<br>• Controller to act as repository of all digital signature certificates (Section 20) |

# IT Act and its provisions

| Chapter | Coverage |
|---|---|
| Chapter IX & XI | • Data Protection (Sections 43 & 66, 66B, 66C, & 66D)<br>• Various types of computer crimes defined and stringent penalties provided under the Act (Section 43, 43A and Sections 66, 66B, 66C, & 66D, 67, 67A, 67B, 72, 72A)<br>• Appointment of Adjudicating officer for holding inquiries under the Act (Sections 46 & 47) |
| Chapter X | • Establishment of Cyber Appellate Tribunal under the Act (Sections 48-56)<br>• Appeal from order of Adjudicating Officer to Cyber Appellate Tribunal and not to any Civil Court (Section 57)<br>• Appeal from order of Cyber Appellate Tribunal to High Court (Section 62) |

# IT Act and its provisions

| Chapter | Coverage |
|---|---|
| Chapter XI & XII | • Interception of information from computer to computer (Section 69) & Protection System (Section 70)<br>• Act to apply for offences or contraventions committed outside India (Section 75)<br>• Investigation of computer crimes to be investigated by an officer not below the rank of an Inspector<br>• Network service providers not to be liable in certain cases (Section 79) |
| Chapter XIII | • Power of police officers and other officers to enter into any public place and search and arrest without warrant (Section 80)<br>• Offences by the Companies (Section 85)<br>• Constitution of Cyber Regulations Advisory Committee who will advice the Central Government and Controller (Section 88) |

# Key Laws Amended by the IT Act, 2000

## Indian Penal Code (IPC)

- The IPC was amended to include cybercrimes such as identity theft, hacking, publishing obscene material, and cyber fraud.

- New provisions were added to cover offenses like forgery of electronic records and cyber terrorism.

# Key Laws Amended by the IT Act, 2000

## Indian Evidence Act, 1872

- Recognized **electronic records** as valid legal evidence.
- Defined **digital signatures and electronic records** as admissible in court proceedings.

- **Bankers' Books Evidence Act, 1891**
- Allowed **electronic records** maintained by banks to be treated as legal evidence.
- Enabled the use of **computer-generated bank records** in legal proceedings.

## Reserve Bank of India (RBI) Act, 1934

- Empowered the **RBI to regulate electronic fund transfers** and digital banking.

- Allowed **RBI to introduce guidelines for cybersecurity and digital payments**.

# Digital Personal Data Protection Act, 2023 (DPDP Act)

- The **Digital Personal Data Protection Act, 2023 (DPDP Act)** is India's first comprehensive law dedicated to regulating the collection, processing, storage, and transfer of personal data.

- It aims to protect the privacy of individuals while enabling a secure digital economy.

- **To Recognize Privacy as a Fundamental Right**

- **To Regulate Data Processing in the Digital Era and address increasing concerns over data misuse.**

- **To Align with Global Standards such as the GDPR (General Data Protection Regulation) of the EU.**

# Key Features of the DPDP Act, 2023

## Applicability

- Applies to **personal data** collected **digitally** or later digitized.

- Covers **data processing** by Indian entities and foreign entities processing data of Indian citizens.

# Key Features of the DPDP Act, 2023

## Consent-Based Data Processing

- **Explicit Consent:** Organizations must obtain clear and informed consent from individuals before collecting their data.
- **Notice Requirement:** Data processors must inform individuals about the purpose and method of data collection.
- **Right to Withdraw Consent:** Individuals can withdraw their consent at any time.

# Key Features of the DPDP Act, 2023

## Rights of Individuals

- **Right to Access:** Individuals can request details of their personal data held by an entity.
- **Right to Correction and Erasure:** Users can correct or delete their data.
- **Right to Grievance Redressal:** Users can file complaints regarding misuse or violations.

# Key Features of the DPDP Act, 2023

## Obligations of Data Processors (Companies/Organizations)

- **Minimization Principle:** Companies should collect only necessary data.
- **Storage Limitation:** Data should not be retained beyond its required purpose.
- **Security Measures:** Companies must implement safeguards to protect personal data.
- **Breach Notification:** In case of a data breach, organizations must notify affected individuals and the **Data Protection Board of India**.

# Key Features of the DPDP Act, 2023

## Data Localization & Cross-Border Data Transfers

- The Act allows cross-border data transfers to **approved countries**, as designated by the government.

- Certain **sensitive data categories** may have stricter storage requirements.

# Key Features of the DPDP Act, 2023

## 6. Data Protection Board of India (DPBI)

- A regulatory body established to **monitor compliance, investigate violations, and impose penalties**.

## 7. Penalties for Non-Compliance

- **Up to ₹250 crore** for major violations.
- **₹200 crore** for failure to prevent personal data breaches.

# IT Act vs DPDP Act

| Feature | IT Act, 2000 | DPDP Act, 2023 |
|---|---|---|
| **Purpose** | Governs cyber activities, electronic commerce, and cybercrimes. | Focuses solely on personal data protection and privacy. |
| **Scope** | Covers electronic records, digital signatures, cybercrimes, and intermediary liability. | Regulates the collection, processing, and transfer of personal data. |
| **Privacy Protection** | Has limited provisions (e.g., Section 43A for compensation in case of data breaches). | Introduces strict rules for personal data collection, consent, and processing. |
| **Penalties** | Imposes fines and imprisonment for cybercrimes. | Imposes heavy fines (up to ₹250 crore) for violations of data protection rules. |
| **Data Localization** | No mandatory data localization requirements. | Requires sensitive data to be stored in India under certain conditions. |

# Digital Signature and the Indian IT Act

- A **digital signature** is an electronic method of verifying the authenticity and integrity of a digital document, message, or transaction.

- It ensures that the sender is legitimate and that the content has not been altered.

- The Information Technology Act (IT Act) of 2000 allows electronic signatures to be used in India and gives them the same legal status as handwritten signatures.

# Key Provisions Related to Digital Signatures in the IT Act, 2000:

- **Legal Recognition of Digital Signatures** (Section 5)

✓ Digital signatures are legally recognized for authentication of electronic records.

✓ It ensures that electronic documents signed with digital signatures are legally valid.

- **Use of Asymmetric Cryptography (Section 3)**

✓ Digital signatures must be created using an asymmetric cryptosystem and a hash function.

✓ This ensures security and integrity in electronic communication.

## Key Provisions Related to Digital Signatures in the IT Act, 2000:

- **Certifying Authorities (Sections 17-34)**

✓ Certifying Authorities (CAs) are entities authorized by the Controller of Certifying Authorities (CCA) to issue digital signature certificates.

✓ CAs verify identities and issue users with Digital Signature Certificates (DSCs).

- **Penalties for Misuse (Sections 65-72A)**

✓ Unauthorized access, fraud, and misuse of digital signatures attract penalties and imprisonment.

# How do digital signatures work in India?

- To create a digital signature, you need a Digital Signature Certificate (DSC) from a licensed Certifying Authority (CA)
- You can use an electronic authentication technique, like Aadhaar e-KYC or PAN-based e-KYC, to sign documents
- The IT Act provides for the Controller of Certifying Authorities(CCA) to license and regulate the working of Certifying Authorities.
- The Certifying Authorities (CAs) issue digital signature certificates for users' electronic authentication. https://cca.gov.in/

# How do digital signatures work in India?

- The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under section 17 of the Act for purposes of the IT Act

- The Controller of Certifying Authorities (CCA) has established the **Root Certifying Authority (RCAI)** of India under section 18(b) of the IT Act to **digitally sign the public keys of Certifying Authorities (CA)** in the country.

- The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA.

- The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the CAs in the country.

# Licenced CA's


SAFE SCRYPT
the confidence to do more

IDRBT

(n)Code Solutions
e-Safe . e-Secure . e-Sure . Licensed Certifying Authority

emudhra
Trust Delivered

सी-डैक
CDAC

Capricorn
Identity Services Pvt. Ltd.

protean
Change *is* growth

VSIGN

Indian Air Force

CSC
e-Governance Services India Limited

RajCOMP Info Services Ltd.
(formerly RajCOMP)
(A Government of Rajasthan Undertaking)
RISL

INDIA ARMY

ID Sign

CDSL VENTURES LIMITED

Pantasign

XtraTrust
TRUST UPDATED

# Electronic Signatures (E-Signatures) and Certificate-Based Digital Signatures

- Both **Electronic Signatures (E-Signatures)** and **Certificate-Based Digital Signatures** are used for authentication in electronic transactions.

**Electronic Signatures (E-Signatures)**

- Can be as simple as typing a name, inserting an image of a signature, or using a stylus on a touchscreen.
- Includes OTP-based Aadhaar authentication (e.g., Aadhaar eSign in India).
- May not always be cryptographically secure but can be legally binding.
- Less secure than digital signatures but convenient for everyday transactions

# Certificate-Based Digital Signatures

- A **Digital Signature** is a type of **Electronic Signature** that provides a higher level of security and is created using **cryptographic algorithms**.
- Uses Public Key Infrastructure (PKI) for encryption and authentication.
- Requires a Digital Signature Certificate (DSC) issued by a Certifying Authority (CA).
- Ensures integrity (document remains unaltered), authenticity (proves the signer's identity), and non-repudiation (prevents denial of signing).
- Used in legally binding documents, contracts, and government filings.

# Public Key Infrastructure (PKI) Framework

- **Public Key Infrastructure (PKI)** is a **framework for handling digital certificates and public-key encryption**, ensuring the secure transfer of information.

- It is used for **authentication, encryption, and ensuring data integrity** in digital systems.

- From **secure email, internet banking, to e-commerce**, PKI enables the **creation, management, distribution, and revocation of digital certificates**—assuring that all parties involved in communication are legitimate and trustworthy. (https://emudhra.com/ )

# Key Components of PKI

## Digital Certificates

- Digital certificates serve as electronic IDs, linking a public key to the identity of an individual, organization, or device.

Each certificate includes:

- Name of the holder
- Public key
- Certificate expiration date
- Digital signature of the Certificate Authority (CA)

The **CA** is a trusted third party that issues and manages digital certificates. Examples: **eMudhra, Sify, NIC, Verisign, DigiCert**.

# Asymmetric Cryptography (Public & Private Keys)

- PKI relies on public-key cryptography (asymmetric encryption).
- Each user has a Public Key (shared) and a Private Key (kept secret).
- Data encrypted with a public key can only be decrypted with the corresponding private key, and vice versa.
- Used in digital signatures and secure communication (e.g., HTTPS, SSL/TLS).

# Public-Key Certificate

- An **X.509 Public-Key Certificate** is a **digital certificate** that follows the **X.509 standard** for **public key infrastructure (PKI)**.
- It is used to authenticate identities and establish **secure communication** using **digital signatures and encryption**.
- An X.509 Certificate contains information about the certificate subject and the certificate issuer (the CA that issued the certificate).
- A certificate is encoded in Abstract Syntax Notation One (ASN.1).
- **Abstract Syntax Notation One (ASN.1)- a** standardized way to define the structure of data used in **Public Key Infrastructure (PKI)**.

# Key Components of PKI

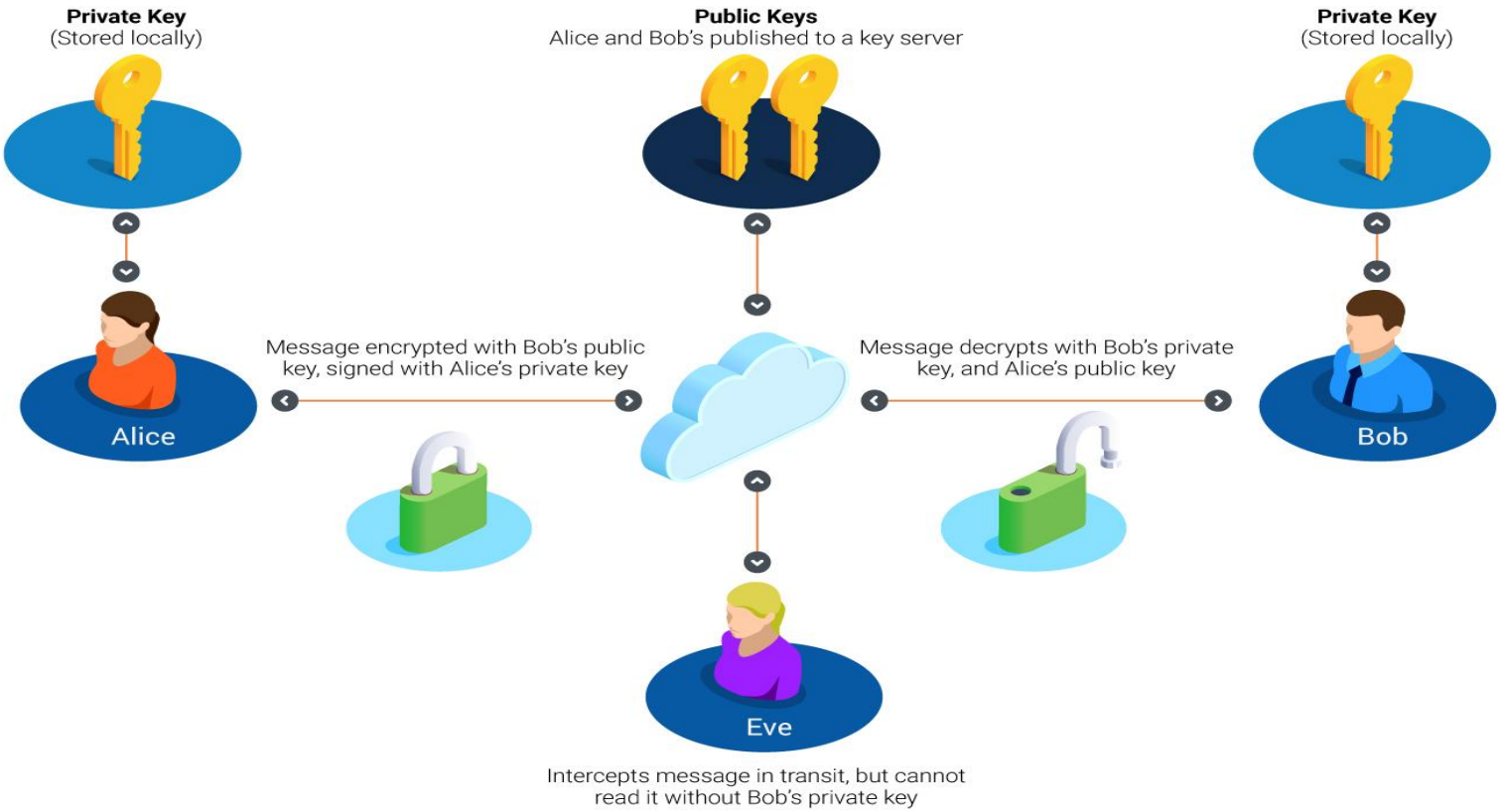
- **Registration Authority (RA)** - The **RA** acts as an intermediary between users and the CA.

- **Certificate Repository**

  - A public directory where issued certificates are stored for verification.

  - Users and applications can access the repository to verify the authenticity of a digital certificate.

# How is Data Encrypted with PKI?




https://www.globalsign.com/en/blog/understanding-pki-overview-and-key-concepts

# Use in Legal Proceedings

- **Admissibility as Evidence**: Digital signatures are admissible as evidence in legal proceedings, provided they meet the conditions set forth in the IT Act. This includes ensuring the integrity and authenticity of the electronic record

- **Non-Repudiation**: Digital signatures provide non-repudiation, meaning the signer cannot deny having signed the document, which is crucial for legal and financial transactions

## Government and Business Adoption

- **E-Governance**: The Indian government extensively uses digital signatures for various e-governance initiatives, including filing tax returns, applying for licenses, and other administrative processes

- **Business Transactions**: Businesses use digital signatures to streamline processes such as contract signing, invoicing, and approvals, enhancing operational efficiency and reducing reliance on physical paperwork

# Section 73: Penalty for Publishing a Digital Signature Certificate with False Particulars

- If a person knowingly publishes a Digital Signature Certificate (DSC) that contains false information or does not belong to them, they are liable for penalties under this section.

A person or entity may be penalized if they:

1. **Publish a DSC with false details**, knowing it is incorrect.
2. **Publish a DSC without authorization** (e.g., using someone else's DSC fraudulently).
3. **Fail to verify certificate details** before publishing, leading to misleading information.

➢ **Fine up to ₹1,00,000 (1 lakh INR). Imprisonment up to 2 years. Or both, depending on the severity of the fraud.**

# Section -74

- Section 74 of the **Information Technology (IT) Act, 2000** deals with **fraudulent publication or use of Digital Signature Certificates (DSCs) or electronic records**.
- It punishes anyone who **knowingly creates, publishes, or misuses a DSC for fraudulent purposes**.

**Example Scenarios of Section 74 Violations in DSCs**

**Forgery of DSC:** A fraudster **creates a fake DSC** and signs documents to obtain loans.
**Unauthorized Use:** A company **uses an employee's DSC without permission** to sign legal agreements.
**Tampering with DSC Information:** Someone **modifies details in a DSC** and submits it for official use.

# Amendments and Updates

## IT (Amendment) Act, 2008

- Introduced provisions for data breaches, identity theft, and cyber-terrorism.
- Defined "sensitive personal data" and imposed stricter obligations on companies.
- Expanded penalties for sending offensive messages, publishing obscene content, and identity fraud.

# Cybercrime and Punishment

## Cheating by Impersonation (Section 66D)

**Crime:** Creating fake profiles, phishing, or impersonating someone online to commit fraud.

**Punishment:**

- **Fine up to ₹1 lakh**.
- **Imprisonment up to 3 years**.

**Example:** A scammer pretending to be a bank officer and stealing OTPs.

# Cybercrime and Punishment

## Hacking & Data Theft (Section 43 & 66)

- ✓ **Crime:** Unauthorized access, hacking, data theft, or damaging computer systems. **Punishment: Fine up to ₹5 lakh**.
- ✓ **Imprisonment up to 3 years**.
- ✓ **Example:** Hacking into a company's database and stealing customer details.

# Cybercrime and Punishment

## Identity Theft (Section 66C)

- ✓ **Crime:** Fraudulent use of someone's **password, digital signature, or biometric data**.
- ✓ **Punishment: Fine up to ₹1 lakh**.
- ✓ **Imprisonment up to 3 years**.
- ✓ **Example:** Using another person's Aadhaar details to apply for a loan.

# E-Commerce & Digital Payment Fraud (Section 66D & Section 84C)

- **Section 66D**: Covers **cheating by impersonation using digital means** (e.g., fake e-commerce websites, fake payment links).

- **Section 84C**: Punishes the **creation or distribution of malicious software** (e.g., ransomware, spyware).

- **Penalty**: **Up to 7 years imprisonment + fine**.

# Cyber Terrorism (Section 66F)

- **Offense**: Committing acts that threaten the unity, integrity, security, or sovereignty of India using computers or communication devices.

- **Penalty**: Imprisonment for life

# Tampering with Computer Source Documents (Section 65)

- **Definition**: Tampering with or altering computer source documents without authorization.

- **Relevance**: This provision protects the integrity of software and other digital assets, which are critical for the functioning of various digital services

# Violation of Privacy (Section 66E)

- **Definition**: Capturing, publishing, or transmitting images of a person without their consent.

- **Relevance**: This provision addresses privacy violations, particularly in the context of the increasing use of smartphones and social mediaa

# Intermediary Liability (Section 79)

- **Offense**: Failure of intermediaries to exercise due diligence and comply with government requests to remove unlawful content.

- **Penalty**: Intermediaries may face penalties as prescribed by the government, including fines and other sanctions

- Telecom service providers, web-hosting service providers, search engines, online payment sites, online marketplaces, and social media platforms

# Intermediary Guidelines and Digital Media Ethics Code, 2021

- The 2021 guidelines introduced additional responsibilities for intermediaries, including:
- Appointing a Chief Compliance Officer, a Nodal Contact Person, and a Resident Grievance Officer.
- Implementing a grievance redressal mechanism to address user complaints.
- Ensuring traceability of the originator of information on their platforms

# Impact of ITA 2008 on Today's Digital Economy

- **Stronger Cybersecurity Laws**: Stricter penalties deter hackers & fraudsters.
- **Protection Against Digital Crimes**: Covers modern cyber threats like identity theft & financial fraud.
- **Regulation of Digital Transactions**: Essential for e-commerce, fintech, and banking security.
- **Better Law Enforcement Tools**: Government agencies can now track cybercriminals more effectively.

# Cyberlaw, Technology and Students: Indian Scenario

- Most technology students have either nil or low exposure to law, and most law students have only limited exposure to information technology.

- A computer science-stream student in a college is taught how to develop programs that can automatically transmit data across the Internet riding on a TCP/IP packet, without alerting him on cybercrimes such as hacking or virus introduction.

- The topic of *secure coding* is not included in most syllabi.

- The Law students should be taught about Trade Marks and Copyrights without recognizing their implications on the electronic documents.

- Thus, neither the technologist nor the lawyer is trained in his formative years to understand cyberlaw.

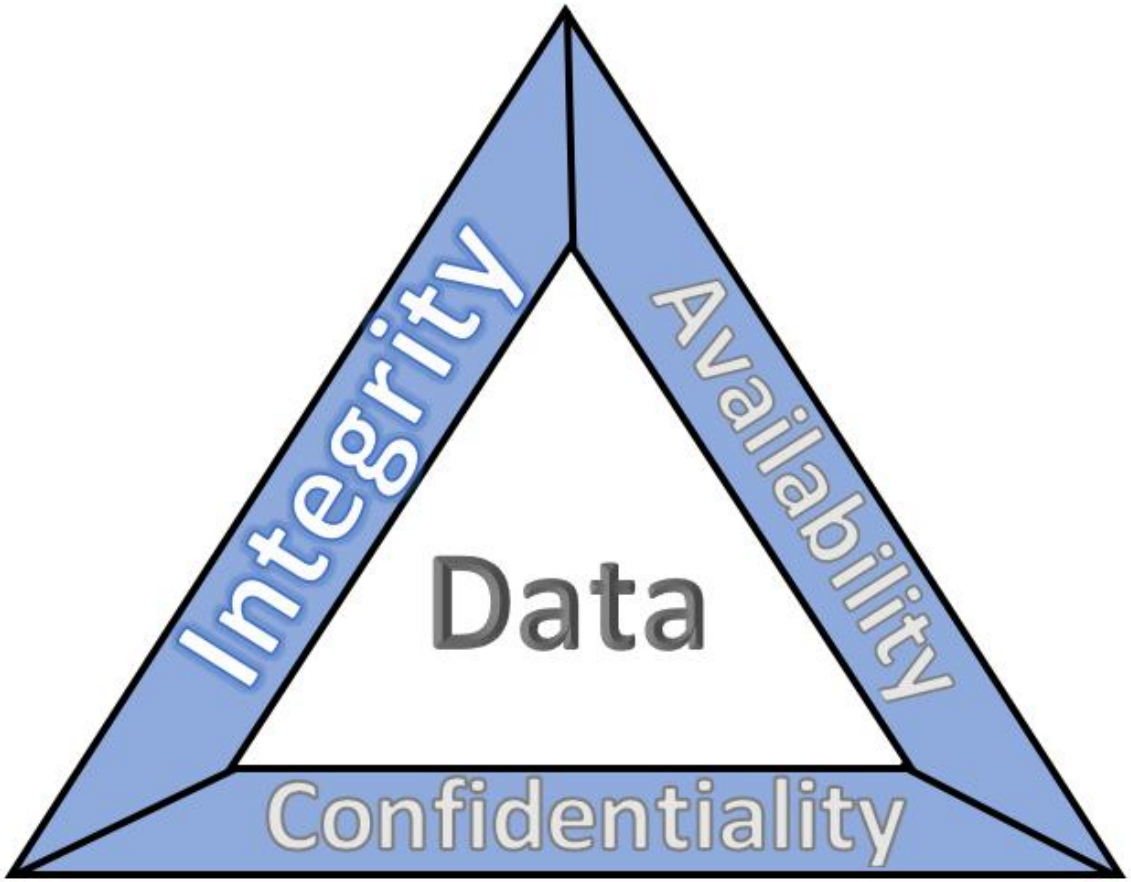
## Some key points on how cyberlaw impacts technology and students:

- **Awareness and Education**
- **Protection Against Cyberbullying**
- **Data Privacy and Security**
- **Ethical Use of Technology**
- **Intellectual Property Rights**

**Respect for IP**: Cyberlaw educates students about respecting intellectual property rights, including copyright, trademarks, and patents. This is particularly important for students involved in creative fields such as writing, music, and **software development**

**Plagiarism Prevention:** Understanding the legal consequences of plagiarism encourages students to produce original work and properly cite sources.

# CIA Traid



# Confidentiality

- **Definition**: Ensures that information is accessible only to those authorized to have access.
- **Key Concepts**:
  - **Encryption**: Protects data by converting it into a coded format that can only be read by someone with the decryption key.
  - **Access Control**: Limits access to information based on user roles and permissions.
  - **Authentication**: Verifies the identity of users before granting access to sensitive information.
- **Examples**: Password protection, biometric verification, and secure communication channels.

# Integrity

**Definition:** Ensures that information is accurate and complete and has not been tampered with.

**Key Concepts:**

- Hashing: Generates a unique hash value for data, which can be used to verify its integrity.
- Checksums: Simple error-detection schemes that ensure data has not been altered during transmission.
- Digital Signatures: Provide a way to verify the authenticity and integrity of a message or document.

**Examples:** Data validation, version control, and audit trails.

# Availability

**Definition**: Ensures that information and resources are available to authorized users when needed.

**Key Concepts**:

- **Redundancy**: Involves having backup systems in place to ensure availability in case of failure.
- **Disaster Recovery**: Plans and processes to recover data and systems after a disruption.
- **Load Balancing**: Distributes workloads across multiple systems to ensure no single system is overwhelmed.

**Examples**: Regular backups, failover systems, and network redundancy.

# Implementing the principles of the CIA Triad

## Confidentiality

- **Data Encryption:** Use strong encryption methods to protect sensitive data both in transit and at rest. This ensures that even if data is intercepted, it cannot be read without the decryption key.

- **Access Control:** Implement robust access control mechanisms, including role-based access control (RBAC) and multi-factor authentication (MFA), to ensure that only authorized individuals can access sensitive information.

- **Data Classification**: Categorize data based on its sensitivity and apply appropriate security measures for each category. This helps in prioritizing protection efforts.

- **Employee Training:** Conduct regular training sessions to educate employees about the importance of data confidentiality and best practices for protecting sensitive information

# Implementing the principles of the CIA Triad

## Integrity

- **Hashing:** Use cryptographic hash functions to generate unique hash values for data. This helps in verifying the integrity of data by comparing hash values before and after transmission.

- **Digital Signatures**: Implement digital signatures to ensure the authenticity and integrity of electronic documents. This provides a way to verify that the document has not been altered.

- **Version Control:** Use version control systems to track changes to data and documents. This helps in maintaining the integrity of data by allowing organizations to revert to previous versions if necessary.

- **Regular Audits:** Conduct regular audits and integrity checks to identify and address any unauthorized changes to data.

# Implementing the principles of the CIA Triad

## Availability

- **Redundancy:** Implement redundancy measures such as backup systems, failover mechanisms, and redundant network connections to ensure continuous availability of data and services.
- **Disaster Recovery Plan:** Develop and regularly update a disaster recovery plan to ensure quick recovery of data and systems in case of a disruption.
- **Load Balancing:** Use load balancing techniques to distribute workloads across multiple servers, preventing any single server from becoming a bottleneck.
- **Regular Maintenance**: Perform regular maintenance and updates on hardware and software to prevent unexpected failures and ensure optimal performance

# E-Commerce Platforms

Online marketplaces implement encryption and access controls to protect customer information (**confidentiality**)

Use version control and regular audits to maintain data **integrity**

Ensure high **availability** through load balancing and redundant network connection.

# Healthcare Organizations

- Healthcare providers use encryption and access controls to protect patient data (**confidentiality**)
- Maintain accurate medical records through hashing and digital signatures (**integrity**)
- Ensure **availability** of critical health information through backup systems and disaster recovery plans

# Financial Institutions

- Banks and financial institutions prioritize **confidentiality** by using encryption and access controls to protect customer data.

- They also implement **integrity** measures such as digital signatures for transaction verification

- **Availability** measures like redundant systems to ensure continuous service.

# Summary

- **The Legal Perspectives - Need of Cyberlaw**
- **The Indian IT Act - Challenges and Consequences**
- **Digital Signature and the Indian IT Act**
- **Cybercrime and Punishment**
- **Cyberlaw - Technology and Students - Indian Scenario –**
- **CIA Triad**