CYBER LAW

Abhishek prajapati
Research scholar
National forensic sciences university

COMPUTER AND ITS COMPONENTS

A computer is an electronic device that accepts input data, processes it according to predefined instructions (programs), and produces output information. It combines hardware (physical components) and software (logical instructions) to perform computational tasks at high speed and with remarkable accuracy.

Core Characteristics:

- Accepts input data through various devices

- Processes data using logical and mathematical operations

- Stores data temporarily or permanently

- Produces meaningful output

- Operates without human intervention once programmed

- Performs tasks with high speed and precision

MAJOR COMPONENTS OF COMPUTER HARDWARE

A. Central Processing Unit (CPU)

The CPU is the core processing element of a computer, often referred to as the "brain" of the computer. It executes program instructions and performs all computational and logical operations.

Functions:

- Fetches program instructions from Random Access Memory (RAM)

- Decodes instructions to understand what operation to perform

- Executes the decoded instructions

- Stores results back in memory

Example: Modern CPUs (Intel Core i9, AMD Ryzen 9) contain multiple cores, allowing parallel processing of multiple instructions simultaneously.

Performance Metrics:

- Clock Speed: Measured in GHz (Gigahertz), determines how many operations per second

- Cores: Number of independent processing units

- Cache Memory: Ultra-fast storage for frequently accessed data

B. Motherboard

The motherboard is the central circuit board that interconnects all computer components, enabling communication between the CPU, RAM, storage devices, and peripherals.

Components and Functions:

- Integrated Circuits (ICs): Contain billions of transistors managing data flow

- Bus Systems: Internal (connects CPU and RAM) and external (connects peripherals)

- Chipset: Controls interactions between CPU and other components

- BIOS/UEFI: Firmware that initializes hardware and boots the operating system

- Power Supply Unit (PSU): Distributes electrical power to all components

Role in System Architecture:

The motherboard acts as the nervous system, transmitting data between components at speeds measured in gigahertz.

C. Random Access Memory (RAM)

RAM is volatile primary memory that temporarily stores data and program instructions actively being used by the CPU.

Key Characteristics:

- Volatile Nature: Loses all data when power is switched off

- Speed: Much faster than secondary storage (nanoseconds vs. milliseconds)

- Addressable: Each memory location has a unique address for direct access

- Capacity: Typical capacities range from 8GB to 128GB in modern computers

Types:

- SDRAM (Synchronous DRAM): Synchronized with CPU clock

- DDR (Double Data Rate): Current standard, DDR4, DDR5 available

- SRAM (Static RAM): Faster but more expensive, used in CPU cache

Example Application in Legal Context:

When forensic investigators analyze computer systems for cyber-crimes, volatile memory analysis is critical—data in RAM that was not properly flushed to disk during an attack can provide evidence of malicious activities.

D. Storage Devices

Primary Functions:

- Permanent data storage

- Program and file retention

- Large-capacity data management

E. Graphics Processing Unit (GPU)

Definition: Specialized processor optimized for rendering graphics and performing parallel computations on multiple data sets simultaneously.

Functions:

- Renders images and videos

- Performs machine learning computations

- Accelerates scientific calculations

- Supports cryptocurrency mining (relevant to cybercrime investigations)

Relevance to Cyber Law:

GPUs are frequently exploited for unauthorized cryptocurrency mining (cryptojacking), representing a significant cyber-crime trend.

F. Power Supply Unit (PSU)

Definition: Converts AC electrical power to regulated DC power for computer components.

Specifications:

- Wattage capacity (500W to 1200W typical)

- Efficiency ratings (80 Plus Bronze, Silver, Gold)

- Protection mechanisms (overvoltage, overcurrent protection)

G. Cooling Systems

Components:

- Air Cooling: Fans that circulate air through heatsinks

- Liquid Cooling: Circulating coolant through water blocks

Importance: Prevents thermal throttling and component damage; critical in forensic evidence preservation.

PERIPHERAL DEVICES

Input Devices:

- Keyboard, Mouse, Touchpad

- Microphone, Scanner

- Biometric readers (fingerprint scanners, face recognition)

Output Devices:

- Monitor/Display

- Speakers/Headphones

- Printers

Storage Peripherals:

- External hard drives

- USB flash drives

- Optical disc drives

COMPUTER ARCHITECTURE MODELS

Von Neumann Architecture:

The fundamental model consisting of:

1. Memory Unit (stores data and instructions)

2. Control Unit (directs operations)

3. Arithmetic Logic Unit (performs calculations)

4. Input/Output Systems

Example Application: Understanding this architecture is essential in analyzing malware behavior, as malware exploits memory management and instruction execution vulnerabilities.

STORAGE MEDIA AND DEVICES

Classification of Storage Media

Storage media are classified based on:

1. Access Method (Sequential vs. Random access)
2. Storage Medium (Magnetic, Optical, Electronic)
3. Volatility (Volatile vs. Non-volatile)
4. Permanence (Temporary vs. Permanent)

PRIMARY STORAGE (VOLATILE MEMORY)

RAM - Random Access Memory

Characteristics:

- Fastest storage medium; - Loses data on power loss

- Required for active computing; - Access time: Nanoseconds

- Cost: Higher per unit

Variants:

- SDRAM, DDR, DDR2, DDR3, DDR4, DDR5

- Each generation provides increased speed and bandwidth

SECONDARY STORAGE (NON-VOLATILE)

A. Hard Disk Drives (HDD)

Definition: Mechanical storage devices using rotating magnetic platters and read/write heads.

Technical Specifications:

- Storage Capacity: 1TB to 14TB

- Speed: 5400 to 7200 RPM (Rotations Per Minute)

- Access Time: 5-10 milliseconds

- Data Transfer Rate: 100-250 MB/s

Advantages:

- Cost-effective per gigabyte; - Large storage capacity; - Suitable for bulk data storage

Disadvantages:

- Slower than SSDs; - Mechanical failure susceptibility; - More power consumption

B. Solid State Drives (SSD)

Definition: Storage devices using flash memory with no moving parts, providing faster data access.

Technical Specifications:

- Storage Capacity: 256GB to 8TB

- Access Time: < 1 millisecond

- Data Transfer Rate: 500 MB/s to 7000+ MB/s (NVMe)

- Speed: 50-100 times faster than HDD

Types:

- SATA SSD: Legacy interface, ~550 MB/s

- NVMe (M.2): Modern protocol, multi-GB/s speeds

Advantages:

- Superior speed and performance; - No mechanical failures; - Better power efficiency; - Durability in physical conditions

Disadvantages:

- Higher cost per gigabyte; - Write endurance limitations; - Data recovery difficulty if failed

C. Hybrid Drives (SSHD)

Definition: Combines SSD and HDD technologies within a single unit.

Configuration:

- Small SSD portion (8-32GB): Frequently accessed data

- Larger HDD portion (1-2TB): Bulk storage

- Intelligent caching algorithm selects what to cache

Use Case: Budget-conscious users seeking compromise between speed and capacity.

OPTICAL STORAGE DEVICES

A. Compact Disc (CD)

Specifications:

- Capacity: 700 MB

- Technology: Laser-read pits on polycarbonate substrate

- Types: CD-ROM (read-only), CD-R (write once), CD-RW (rewritable)

- Lifespan: 10-50 years depending on quality

Data Structure:

- Single spiral track (1.6 km long); - Data read at constant linear velocity; - Error correction code built-in

Legal Use:

- Software distribution; - Data archival; - Legal evidence storage (less common now)

B. Digital Versatile Disc (DVD)

Specifications:

- Capacity: 4.7GB (single layer), 8.5GB (dual layer)

- Advantages: 7x storage over CD

- Types: DVD-ROM, DVD-R, DVD-RW, DVD+RW

Technical Improvement:

- Smaller pits and closer track spacing than CD

- Shorter wavelength laser (650nm vs. 780nm)

Application: Video distribution, high-capacity backups.

C. Blu-ray Disc (BD)

Specifications:

- Capacity: 25GB (single layer), 50GB (dual layer), 100GB (quadruple layer)

- Technology: Blue laser (405nm wavelength)

- Video Format: Supports 4K resolution

Advantages:

- Massive storage capacity

- High-definition content support

- Better archival longevity

Cyber Forensics Application:

Blu-ray media increasingly used for long-term evidence archival due to stability.

FLASH MEMORY DEVICES

USB Flash Drives

Definition: Portable storage using flash memory with USB interface.

Characteristics:

- Capacity: 32GB to 1TB+

- Speed: 10-100 MB/s typically

- Portability: Pocket-sized, lightweight

- Durability: No moving parts, shock-resistant

Flash Memory Types:

- TLC (Triple Level Cell): 3 bits per cell, more capacity, slower

- MLC (Multi-Level Cell): 2 bits per cell, balanced

- SLC (Single Level Cell): 1 bit per cell, fastest, less capacity

Cyber Crime Connection:

USB flash drives are primary vectors for:

- Malware distribution

- Data exfiltration from enterprises

- Evidence removal during investigations

Data Recovery Challenges:

Flash memory stores charge on floating gates; once discharged, recovery requires electron microscopy analysis.

SD Cards and MicroSD Cards

Specifications:

- Capacity: 32GB to 1TB

- Speed Classes: U3, V90 for consistent performance

- Use Cases: Cameras, smartphones, portable devices

Advantages:

- Smaller footprint than USB drives

- Hot-swappable without system restart

- Integrated with mobile devices

CLOUD AND NETWORK STORAGE

Cloud Storage

Definition: Data stored on remote servers accessible via internet connectivity.

Technologies:

- Redundancy: Data replicated across multiple data centers

- Scalability: Storage expands dynamically

- Accessibility: Access from any device globally

Examples: Amazon S3, Microsoft Azure, Google Cloud Storage

Cyber Law Implications:

- Jurisdiction Issues: Data may be stored in multiple countries

- Subpoena Compliance: Service providers must preserve data per legal requirements

- Privacy Regulations: GDPR, DPDP Act apply to cloud data storage

- Data Breach Notification: Mandatory reporting of unauthorized access

Network Attached Storage (NAS)

Definition: Storage device connected to network, accessible by multiple computers.

Characteristics:

- Architecture: Dedicated operating system for file management

- RAID Support: Data redundancy and performance optimization

- Multiple Protocols: NFS, SMB, AFP

Enterprise Use: Centralized backup and collaborative data access.

Storage Area Network (SAN)

Definition: High-speed network providing block-level storage access to servers.

Technology:

- Connectivity: Fibre Channel or iSCSI protocols

- Performance: Very high throughput for enterprise applications

- Scalability: Large storage pools for data centers

Forensic Challenge: SAN evidence collection requires specialized expertise and tools.

DATA RECOVERY AND FORENSIC IMPLICATIONS

Physical Destruction:

- HDD: Platters can be damaged; mechanical shredding standard

- SSD: NAND flash degradation over time; secure erase becomes permanent after 10-15 years

- Optical: Surface damage prevents laser reading

Logical Recovery:

- Deleted files remain recoverable until overwritten

- TRIM and GARBAGE COLLECTION decrease recovery possibility

- Multiple passes may be required for thorough deletion

Cyber Crime Investigation:

- Chain of custody documentation mandatory

- Write-blocking devices prevent evidence tampering

- Forensic imaging creates bit-for-bit copies for analysis

CATEGORIES AND CLASSIFICATION OF CYBERCRIME

Cybercrime encompasses illegal activities carried out using computers, networks, or the internet. It includes both:

1. Crimes Against Computers: Direct attacks on computer systems and infrastructure

2. Crimes Using Computers: Traditional crimes committed through digital means

CATEGORY 1: CYBERCRIMES AGAINST INDIVIDUALS

These crimes target personal data, privacy, and dignity of individuals.

Subcategories:

A. Email Spoofing

- Definition: Forging email headers to appear from legitimate sources

- Method: Manipulation of SMTP (Simple Mail Transfer Protocol) headers

- Example: Fraudulent emails appearing from banks requesting account verification

- Legal Provision: Section 66C, 66D IT Act 2000

- Penalties: Up to 3 years imprisonment or ₹1 lakh fine

B. Phishing

- Definition: Fraudulent solicitation of sensitive information through deceptive means
- Mechanism:
  - Creation of fake websites mimicking legitimate organizations
  - Tricks users into entering passwords, credit card numbers, or personal data
  - Redirects to malicious sites through URL manipulation
- Variants:
  - Spear Phishing: Targeted at specific individuals with personalized information
  - Whaling: Targets high-level executives
  - Clone Phishing: Creates exact copy of legitimate messages with malicious links
- Example: ICICI Bank Phishing Case—Victim received phishing email requesting banking credentials, lost ₹6.46 lakh
- Legal Framework: Sections 66D, 66E IT Act 2000
- Penalties: Up to 3 years imprisonment and ₹1 lakh fine

C. Spamming

- Definition: Unsolicited bulk electronic communications

- Types:

  - Email spam (the most common form)

  - SMS spam

  - Social media spam

  - Comment spam on websites

- Volume Impact: Over 85% of email traffic is spam globally

- Legal Status: Section 66A (now struck down as unconstitutional); Section 43 provides civil liability

- Business Impact: Estimated annual damage to economy

D. Cyberstalking

- Definition: Repetitive, threatening online harassment causing fear or distress
- Methods:
  - Persistent messaging and contact
  - Public embarrassment through posting personal information
  - Impersonation and identity theft
  - Distribution of intimate images without consent
- Legal Provisions: IPC Section 354D (harassment), IT Act Section 66E
- Penalties: Up to 3 years imprisonment or ₹2 lakh fine

E. Cyber Defamation

- Definition: Publication of false information online that damages reputation
- Elements Required:
  - False statement (truth is complete defense)
  - Intent to harm
  - Public accessibility of the content
  - Actual reputational harm
- Platforms: Social media, blogs, review sites, forums
- Legal Framework: IPC Section 499-500, IT Act Section 43
- Landmark Case: Shreya Singhal v. Union of India (2015)—struck down Section 66A as unconstitutional

F. Cyber Harassment and Bullying

- Definition: Targeted, repeated hostile behavior online causing psychological harm
- Forms:
  - Abusive messages and comments
  - Threatening language
  - Impersonation
  - "Doxxing" (publishing private information)
  - Coordinated harassment campaigns
- Vulnerable Groups: Women, children, minorities
- Legal Provisions: IPC Section 354A (sexual harassment), IT Act Section 66E

CYBERCRIMES AGAINST PROPERTY

These crimes target intellectual property, financial assets, and proprietary information.

Subcategories:

A. Credit Card Fraud

- Definition: Unauthorized use of credit card information for financial gain
- Methods:
  - Card number theft through phishing
  - Skimming devices on ATMs
  - Data breach exploitation
  - Counterfeit card creation
- Example: Pune Citibank Case—Ex-employees defrauded US Citibank customers of ₹1.5 crores
- Legal Provisions: Sections 66C, 66D IT Act; IPC Section 420 (cheating)
- Penalties: Up to 3 years imprisonment and ₹5 lakh fine

B. Intellectual Property Crimes

- Definition: Unauthorized reproduction, distribution of copyrighted/patented digital content

- Forms:

  - Software piracy

  - Movie and music illegal distribution

  - E-book unauthorized copying

  - Patent infringement

- Economic Impact: Estimated annual loss of $250 billion globally

- Legal Framework: Copyright Act 1957, Patents Act 1970

- Enforcement: IIPA (International Intellectual Property Alliance) tracking

C. Internet Auction Fraud

- Definition: Fraudulent transactions on online marketplace platforms

- Scenario: Seller accepts payment but fails to deliver; buyer receives non-genuine product

- Platform Risk: eBay, Flipkart vulnerable areas

- Remedies: Escrow services, buyer protection policies

D. Internet Time Theft

- Definition: Unauthorized use of internet bandwidth/services

- Methods:
  - Unauthorized WiFi network access
  - Bandwidth throttling through compromised devices
  - Service account credential sharing

- Cost to ISPs: Estimated millions annually

CYBERCRIMES AGAINST ORGANIZATIONS

Large-scale attacks targeting corporate infrastructure and sensitive data.

Subcategories:

A. Unauthorized Access (Hacking)

- Definition: Accessing computer systems without authorization
- Technical Methods:
  - Exploiting software vulnerabilities (zero-day exploits)
  - Weak password cracking (brute force, dictionary attacks)
  - Social engineering to obtain credentials
  - Man-in-the-middle attacks
  - SQL injection and command injection
- Motive: Data theft, sabotage, espionage, ransom
- Legal Provision: Section 66 IT Act 2000
- Penalties: Up to 3 years imprisonment and ₹5 lakh fine

B. Denial of Service (DoS) / Distributed Denial of Service (DDoS)

- Definition: Overwhelming systems with requests, denying legitimate users access

- DoS: Single attacker system attacks target

- DDoS: Multiple compromised systems (botnet) attack simultaneously

- Impact:

  - Website unavailability

  - Business revenue loss

  - Service disruption

- 2011-13 Iran DDoS Campaign: Against US Financial Sector—176 cumulative days of attacks, tens of millions in damages

- Legal Status: Section 66 IT Act

- Penalties: Imprisonment and fines

C. Malware Attacks

- Types:
  - Virus: Self-replicating, requires host program
  - Worm: Self-propagating, spreads independently across networks
  - Trojan Horse: Appears legitimate, contains malicious payload
  - Ransomware: Encrypts files, demands payment for decryption
  - Spyware: Monitors and steals user data
  - Rootkit: Provides administrator access, hides from detection
- Propagation: Email attachments, infected websites, removable media, P2P networks
- Detection: Antivirus engines, behavioral analysis, sandboxing
- Legal Provision: Section 66 IT Act

EMAIL BOMBING

- Definition: Overwhelming email system with massive volume of messages

- Method: Automated mass email sending to specific address

- Impact: System crash, denial of service, network congestion

- Legal Status: Section 66 IT Act 2000

SALAMI ATTACK

Definition: Small, repeated unauthorized deductions/alterations accumulating to significant loss

- Example: Bank transfer system skimming fractions of cents from millions of accounts

- Detection Difficulty: Small individual transactions avoid triggers

- Legal Provision: Section 43, 66 IT Act

DATA DIDDLING

- Definition: Unauthorized alteration of data before processing
- Example: Inventory records modification to hide theft
- Impact: False reporting, fraud, compliance violations
- Industry Risk: Finance, healthcare, retail sectors

INDUSTRIAL ESPIONAGE (CYBER)

- Definition: Stealing trade secrets and confidential business information
- Methods: Insider threats, hacking, social engineering, physical theft of devices
- Targets: R&D data, customer lists, strategic plans, pricing information
- Legal Status: Trade Secrets Protection Act, IT Act Section 43

LOGIC BOMBS

Definition: Malicious code triggered by specific conditions/date

- Example: Employee disgruntled before termination embeds code to delete data on their last day

- Detection: Code review, source control monitoring

- Legal Status: Section 66 IT Act

SOFTWARE PIRACY

Definition: Unauthorized copying and distribution of software

- Forms:

  - End-user piracy (home users)

  - Internet piracy (illegal downloads)

  - Business software theft

  - Counterfeit software sales

- Cost: $62.4 billion annually (Business Software Alliance)

- Legal Framework: Copyright Act, DMCA (US), Software Piracy Act

CYBERCRIMES AGAINST SOCIETY / CYBER TERRORISM

Attacks threatening national security, social stability, and critical infrastructure.

A. Cyber Terrorism

- Definition: Using computer systems to achieve political/social objectives through violence and fear

- Characteristics:

  - Ideological motivation; - Targets critical infrastructure

  - Causes mass disruption or loss of life; - Intent to create fear and social disruption

- 2007 Estonia Cyberattacks: Disrupted government, banking, media for 3 weeks

- WannaCry Ransomware (2017): Attributed to North Korea, infected NHS systems globally

- Legal Provision: Section 66F IT Act—Life imprisonment

- International Framework: Budapest Convention, UN regulations

B. HACKING CRITICAL INFRASTRUCTURE

- Infrastructure Types:
  - Power grids and electrical systems
  - Water treatment facilities
  - Transportation networks
  - Healthcare systems
  - Communication networks
- Impact: Loss of life, economic damage, national security threats
- Example: 2015 Ukraine Power Grid Attack—attackers remotely cut electricity to 230,000 people
- Detection and Response: Automated monitoring, incident response teams, backup systems

C. WEBSITE DEFACEMENT / WEB JACKING

- Definition: Unauthorized modification of website content

- Methods: Exploiting web vulnerabilities, obtaining admin access

- Impact: Reputational damage, message spreading, disruption of services

- Famous Examples: Political activism, hacktivist groups, espionage

- Remediation: Rapid website restoration, security patches

D. CYBER WARFARE/STATE-SPONSORED ATTACKS

- Definition: Cyberattacks by nations targeting other nations' infrastructure
- Characteristics:
  - Sophisticated, well-funded operations; - Targets critical national infrastructure
  - Part of military/political strategy; - Often involving espionage components
- Examples:
  - Stuxnet worm (2010)—targeted Iranian nuclear facilities
  - NotPetya (2017)—attributed to Russian military
  - SolarWinds Supply Chain Attack (2020)—attributed to Russian SVR
- International Law: Emerging framework for attributing state responsibility
- Response Mechanisms: Sanctions, counter-attacks, diplomatic action

E. DISTRIBUTION OF OBSCENE MATERIAL

- Definition: Online dissemination of sexually explicit content

- Legal Provision: Section 67 IT Act—Up to 5 years imprisonment and ₹10 lakh fine

- Specific Focus: Protection of minors from exploitation

DEFINITION OF CYBER LAW

Cyber Law is the branch of law dealing with legal issues arising from internet use, digital technology, electronic communications, and cybercrime. It encompasses legislative, regulatory, and case law addressing:

- Data protection and privacy

- Cybersecurity and incident response

- Crime investigation and prosecution

- Intellectual property in digital context

- E-commerce and digital transactions

- Telecommunications regulation

SCOPE OF CYBER LAW

Core Areas:

1. Criminal Law: Prosecution of cybercrimes
2. Civil Law: Disputes, tort liability, damages
3. Administrative Law: Regulatory compliance
4. International Law: Cross-border investigations, treaties
5. Substantive Law: Crime definitions, penalties
6. Procedural Law: Investigation methods, evidence collection, prosecution procedures

PURPOSE AND OBJECTIVES

Primary Objectives:

- Protection: Safeguard individuals and organizations from cyber threats

- Justice: Hold cybercriminals accountable

- Regulation: Establish standards for secure digital practices

- Facilitation: Enable legitimate electronic commerce and communications

- Harmonization: Create international consistency in cyber law

KEY STAKEHOLDERS IN CYBER LAW IMPLEMENTATION

Government Agencies:

- Police (Cyber Crime cells); - Intelligence agencies; - Banking regulators;

- Telecom regulators; - Data protection authorities

Private Sector:

- Technology companies; - Financial institutions

- Healthcare providers; - E-commerce platforms

International Organizations:

- United Nations; - Council of Europe

- International Criminal Police Organization (Interpol)

- Regional organizations (ASEAN, African Union)

INFORMATION TECHNOLOGY ACT, 2000 (INDIA)

Background and Legislative Context

Pre-2000 Scenario:

- No specific legislation for cybercrime in India

- Existing IPC and Evidence Act inadequate for digital crimes

- International treaties lacked implementation mechanism

The Information Technology Act, 2000 (ITA-2000) was enacted as Act No. 21 of 2000 by the Indian Parliament.

Passage and Enactment:

- Passed in budget session of 2000
- Signed by President K.R. Narayanan on May 9, 2000
- Notified on October 17, 2000
- Formulated by group headed by then Minister of IT, Pramod Mahajan

Original Structure:

- 94 sections divided into 13 chapters
- 4 schedules (Schedule 3 and 4 later omitted)
- Applicable to entire India
- Extraterritorial application if Indian computer/network involved

STRUCTURAL ORGANIZATION

Chapters:

1. Preliminary: Definitions and applicability
2. Digital Signatures: Authentication framework, certification authorities
3. Electronic Governance: E-records, digital signatures recognition
4. Security Procedures and Practices: Technical standards
5. Attribution and Acknowledgment: Digital signature requirements
6. Secure Electronic Records: Digital document validity
7. Electronic Contracts: Formation and validity of e-contracts
8. Regulation of Certifying Authorities: Controller of Certifying Authorities (CCA)
9. Adjudication: Civil disputes resolution
10. Offences: Criminal provisions and penalties
11. Miscellaneous: Appeals, penalties, exemptions
12. Cyber Appellate Tribunal: Dispute resolution authority
13. Enhancement of IT Infrastructure: National digital development

KEY CONCEPTS AND DEFINITIONS

Computer Network: Any system of interconnected computers and devices enabling data communication and information sharing.

Computer Data: Information in form of electronic records including text, images, audio, video stored or transmitted through computers.

Computer System: Device or collection of devices including computer programs and data for performing specified functions.

Computer Resource: Hardware, software, data, and network systems (term used broadly in IT Act).

Information: Data in electronic form pertaining to any transaction.

Intermediary: Any entity providing internet/data services, hosting data, or facilitating online transactions. Key provision: Section 79 provides immunity if due diligence exercised and unlawful content promptly removed upon notice.

ADDRESSEE (SECTION 2(1)(B))

Definition: A person who is intended by the sender to receive an electronic record.

Important: The addressee does NOT include any intermediary (middleman or service provider).

Examples:

Email sent from Raj to Priya → Priya is the addressee

A contract sent to XYZ Company → XYZ Company is the addressee

An e-invoice sent to a customer → The customer is the addressee

SUBSCRIBER (SECTION 2(1)(ZG))

Definition: A person in whose name an Electronic Signature Certificate (Digital Signature Certificate) is issued.

Key Point: You become a subscriber only after getting a Digital Signature Certificate from a Certifying Authority.

Who are subscribers?

Chartered Accountants (for filing tax returns)

Company Directors and Secretaries

Bank authorized signatories

Government employees

DIGITAL SIGNATURE (SECTION 2(1)(P))

Definition: Authentication of any electronic record by a subscriber using a special electronic method or code (cryptography).

Key Features: Proves sender's identity, ensures document hasn't been altered, provides legal evidence.

Common Uses:

GST return filing

Income tax e-filing

ELECTRONIC SIGNATURE (SECTION 2(1)(TA))

Definition: Authentication of any electronic record by a subscriber using any electronic technique specified by the government.

Important: BROADER than digital signature. Includes digital signature plus other methods. Can be less secure or more secure.

Types of E-Signatures:

Digital Signature (using cryptography)

Aadhaar eSign (Aadhaar biometric)

PAN eSign (PAN-based signature)

Email signature (typing name in email)

All digital signatures are electronic signatures, but NOT all electronic signatures are digital signatures.

Feature	Electronic Signature	Digital Signature
Definition	Any electronic way to sign	Encrypted signature using cryptography
Technology	Simple methods (typing, images, clicks)	Encryption, digital certificates
Security	Low to moderate	High security with verification
Verification	Not by trusted authorities	By Certificate Authorities

Electronic Signature is the **broader umbrella** term, while Digital Signature is a **specific secure type**.

Feature	Electronic Signature	Digital Signature
Document Integrity	No guarantee against alteration	Ensures integrity with hash function
Legal Validity	Routine transactions only	High-value, sensitive transactions
Cost	Low cost, easy to apply	Higher cost with certificate
Non-repudiation	Signer can deny	Signer cannot deny

MAJOR SECTIONS AND PROVISIONS

A. Civil Liability (Section 43):

Unauthorized Access and Data Interference:

The provision establishes civil liability for:

Action	Damages
Unauthorized access to computer	Up to ₹1 lakh
Data alteration/destruction	Compensation for actual loss
System interference	Compensation for disruption
Denial of service	Compensation for revenue loss
Transmission of malicious code	Compensation for damage

ADJUDICATION PROCESS

Adjudicating officer –Appointed under 46 (1)

- Aggrieved person files complaint with adjudicating officer

- Officer investigates and determines damages

- Maximum compensation limited to ₹1 crore per incident

- Non-criminal remedy; no imprisonment

Example Application: Company discovers unauthorized access to employee database; estimates data protection costs at ₹50 lakh; seeks compensation through adjudication.

PENAL PROVISIONS (SECTIONS 65-74)

Section 65: Tampering with Computer Source Documents

- Offense: Knowingly modifying or destroying source code of programs

- Intent Required: Dishonest or fraudulent

- Penalty: Imprisonment up to 3 years and/or fine up to ₹2 lakh

- Example: Developer modifies banking software code to siphon fund

Section 66: Hacking/Unauthorized Computer Access

- Offense: Knowingly accessing computer systems without authorization
- Requirements:
  - Intentional act
  - Without permission or authority
  - Knowledge of unauthorized nature
- Penalty: Imprisonment up to 3 years and/or fine up to ₹5 lakh
- Landmark Case: First conviction case involved credit card fraud on sony-sambandh.com

Section 66A: Sending Offensive Messages (STRUCK DOWN - 2015)

- Original Provision: Criminalized sending messages through communication service with intent to cause annoyance, inconvenience, insult, injury, etc.

- Landmark Judgment: Shreya Singhal v. Union of India (2015) declared it unconstitutional

- Reasons for Striking Down:

  - Violated Article 19(1)(a) - freedom of speech

  - Too vague and broad

  - Chilled legitimate free speech

  - No requirement for incitement or substantial public harm

  - Susceptible to misuse by authorities

- Impact: Significant precedent protecting online expression in India

Section 66B: Receiving Stolen Computer Property

- Offense: Receiving or retaining stolen computer/communication device with knowledge

- Penalty: Imprisonment up to 3 years and/or fine up to ₹1 lakh

Section 66C: Using Electronic Password of Another Person

- Offense: Dishonestly using another person's computer password or unique identification feature

- Intent Required: Fraudulent or dishonest purpose

- Penalty: Imprisonment up to 3 years and/or fine up to ₹1 lakh

- Application: Identity theft, account takeover crimes

Section 66D: Cheating Using Computer Resource

- Offense: Cheating or defrauding using computer/internet

- Methods: Fake websites, fraudulent transactions, identity spoofing

- Penalty: Imprisonment up to 3 years and/or fine up to ₹1 lakh

- Example: Online romance scams, fake e-commerce sites

Section 66E: Invading Privacy/Publishing Private Images

- Offense: Publishing private images without consent via computer/internet

- Application to Revenge Porn: Distributing intimate images to cause distress

- Penalty: Imprisonment up to 3 years and/or fine up to ₹2 lakh

- Defenses: Legitimate purpose (news reporting, legal proceedings)

Section 66F: Cyber Terrorism

- Definition: Accessing or destroying computer systems to threaten India's sovereignty, security, unity, or integrity

- Intent Required: Disrupting critical infrastructure, causing fear

- Penalty: Life imprisonment (most severe provision)

- Standards: Must meet terrorism threshold (not ordinary hacking)

- International Relevance: Similar to US CFAA provisions

Section 67: Publishing Obscene Material in Electronic Form

- Offense: Publishing obscene material electronically with knowledge

- Intended Audience: Likely to read, see, or hear the material

- Penalty:

  - First conviction: Up to 3 years and/or ₹5 lakh fine

  - Subsequent conviction: Up to 5 years and/or ₹10 lakh fine

Section 67A: Publishing Sexually Explicit Content

- Specific Focus: Images containing sexual acts in electronic form
- Penalty:
  - First offense: Up to 7 years imprisonment and/or ₹10 lakh fine
  - Subsequent offense: Extended penalties

Section 67B: Punishment for Publishing Material Depicting Children in Sexual Acts

- Offense: Publishing or transmitting CSAM (Child Sexual Abuse Material)
- Elements: Must depict actual sexual conduct
- Penalty: Up to 5 years for first offense; up to 8 years for subsequent offenses
- Higher Penalties: If victim under 12 years or material very violent

Section 68: Failure to Comply with Orders

- Offense: Failure to comply with government orders regarding data/documents

- Penalty: Up to 2 years imprisonment and/or ₹1 lakh fine

Section 69: Government Authority for Data Interception

- Grant of Power: Government can direct interception, monitoring, or decryption of data

- Purpose: National security, public order, sovereignty protection

- Requirements: Government notification specifying reasons

- Compliance: ISPs/service providers must facilitate

- Penalty for Non-Compliance: Imprisonment up to 7 years

- Procedural Safeguards: Limited; minimal judicial review required

- Privacy Concerns: Criticized as overly broad surveillance power

Section 69A: Blocking of Information on Internet

- Purpose: Block access to information threatening national security/integrity

- Process: Government issues notification; ISPs must block access

- Penalty for Non-Compliance: Imprisonment up to 7 years and fine

- Impact: Used to block content related to political dissent, activism

- Criticism: Potential for overreach and censorship

Section 69B: Monitoring and Collection of Traffic Data

- Requirement: Agencies must monitor network traffic for cyber security

- Data Collection: Traffic data, communication metadata

- Penalty for Non-Compliance: Imprisonment up to 1 year and/or fine up to ₹1 crore

- Privacy Implications: Large-scale surveillance capability

Section 70: Protection of Critical Information Infrastructure

- Definition: Critical systems whose compromise threatens national security

- Offense: Securing or attempting to secure unauthorized access

- Penalty: Imprisonment up to 10 years (most severe non-terrorist offense)

- Application: Power grids, banking systems, telecommunications

Section 71: Misrepresentation to Controller

- Offense: Providing false information to Certifying Authority

- Penalty: Up to 2 years imprisonment and/or ₹1 lakh fine

Section 72: Breach of Confidentiality and Privacy

- Offense: Disclosing information obtained in official capacity without authorization

- Applicable To: Government employees, service providers

- Penalty: Up to 2 years imprisonment and/or ₹1 lakh fine

- Exception: Disclosure legally required or with authorization

Section 72A: Disclosure in Breach of Lawful Contract

- Offense: Disclosing information in violation of contract terms

- Example: Employee revealing trade secrets

- Penalty: Up to 3 years imprisonment and/or fine up to ₹5 lakh

Section 73: False Digital Signature Certificate

- Offense: Publishing or causing publication of false digital signature certificate

- Penalty: Up to 2 years imprisonment and/or ₹1 lakh fine

Section 74: Publication for Fraudulent Purpose

- Offense: Publishing false digital signature certificate with fraudulent intent

- Penalty: Up to 2 years imprisonment and/or ₹1 lakh fine

AMENDMENTS TO IT ACT, 2000

Major Amendment of 2008

Enacted February 5, 2009, the 2008 Amendment significantly expanded cybercrime provisions:

New Offenses Introduced:

Offense	Section	Penalty
Cheating by personation	66D	3 years/₹1 lakh
Identity theft	66C	3 years/₹1 lakh
Violation of privacy	66E	3 years/₹2 lakh
Cyber terrorism	66F	Life
Obscene content children	67A	7 years/₹10 lakh

Interception Powers Expanded:

- Section 69 strengthened with decryption authority
- Section 69A enabled blocking of public access
- Section 69B added traffic data monitoring

CSAM Provisions Enhanced:

- More severe penalties for child-related content
- Recognition of computer-generated exploitative material
- Extended scope to grooming, solicitation

AMENDMENT OF 2009

Minor adjustments implementing 2008 amendments and addressing implementation issues.

IT Rules 2021 (Secondary Legislation)

Intermediary Guidelines and Digital Media Ethics Code Rules, 2021

Strengthens regulation of social media platforms and digital intermediaries:

KEY REQUIREMENTS

1. Grievance Redressal Mechanism:

- Designated grievance officer; - Response within 24 hours for unlawful content complaints; - Resolution within 15 days

2. Content Removal:

- Removal of offensive/illegal content within 24-72 hours of notice; - No hosting of content violating laws

3. Due Diligence:

- Regular monitoring for unlawful content; - Privacy protection measures; - Transparency reports published quarterly

4. User Verification:

- Identification of users engaged in severe violations; - Disclosure to law enforcement when legally required

Impact:

- Increased platform liability for third-party content

- More stringent compliance requirements

- Balancing act between free speech and regulation

JURISDICTIONAL SCOPE

Territorial Application:

- Act applies throughout India

- Extraterritorial effect: If computer/network in India involved, even if accused foreign national

Jurisdiction for Prosecution:

- Crime venue where computer system located (committed)

- Crime venue where result felt (data accessed from)

- Multiple jurisdictions possible if data in multiple states

International Coordination:

- Mutual legal assistance treaties with multiple countries

- Interpol coordination for international cybercriminals

- Extradition treaties for severe crimes

INTERNATIONAL CYBER LAWS AND TREATIES

Budapest Convention on Cybercrime (2001)

The first comprehensive international treaty on cybercrime, established by the Council of Europe in 2001. Currently has 68+ signatory nations.

Primary Objectives:

1. Harmonize cybercrime laws across nations

2. Establish procedural mechanisms for investigation

3. Create framework for international cooperation

4. Ensure rule of law and human rights protection

A. SUBSTANTIVE CRIMINAL LAW PROVISIONS

Offenses Against Confidentiality, Integrity, Availability:

1. Illegal Access: Accessing computer systems without right

   - May require intentional infringement of security measures; - Dishonest intent or obtaining computer data

2. Illegal Interception: Capturing data transmissions without authorization

   - Focus: Electromagnetic emissions, network traffic; - Methods: Wire-tapping, packet sniffing

3. Data Interference: Unauthorized access, alteration, deletion of computer data

   - Includes introduction of corrupted data; - Reckless or intentional modification

4. System Interference: Serious hindrance to system operation

   - Input, transmission, damage, deletion of data; - Intent to obstruct or substantially prevent legitimate use

5. Misuse of Devices: Production, sale, procurement of hacking tools

   - Includes passwords, hacking software; - Parent provision for computer-related offenses

Intellectual Property and Fraud Offenses:

6. Computer-Related Forgery: Creating, altering digital records

- False digital signatures
- Tampered certificates
- Fraudulent digital documents

7. Computer-Related Fraud: Causing loss through deception/manipulation

- False/misleading input to computer systems
- Identity spoofing
- Financial institution fraud

Content-Related Offenses:

8. Child Pornography Offenses:

- Production, distribution, possession of CSAM
- Knowledge of content illegal required
- Applies to computer-generated material indistinguishable from real children

9. Copyright Infringement: Unauthorized reproduction/distribution

- Digital piracy
- Reverse engineering of protected software

B. PROCEDURAL POWERS AND SAFEGUARDS

Investigation Tools (Subject to Rule of Law Constraints):

1. Expedited Preservation of Stored Computer Data

   - Rapid procedures to preserve volatile evidence

   - ISP cooperation requirements

   - 24-48 hour preservation timeline

2. Expedited Disclosure of Traffic Data

   - Subscriber information disclosure

   - Communications metadata

   - Timing restrictions to ensure relevance

3. Production Orders

- Compel disclosure of computer data held by service providers
- Addressed to person in control of information
- Balance with privacy rights

4. Search and Seizure

- Judicial authorization for computer system searches
- Seizure of computer hardware/storage media
- Forensic analysis of digital evidence

5. Real-Time Collection of Traffic Data

- Monitoring of data transmission
- Limited to specific suspect
- Judicial authorization required

6. Interception of Content Data

- Wiretapping with authorization
- Access to communications content
- Highest privacy restriction level

C. INTERNATIONAL COOPERATION FRAMEWORK

1. Extradition for Cybercrime

- Recognition of cybercrime as extraditable offense; - Mutual extradition agreements; - Procedures for surrender of suspected cybercriminals

2. Mutual Legal Assistance (MLA)

- Evidence gathering between signatory states; - Witness testimony transmission; - Document authentication; - Confidentiality protections

3. Spontaneous Information Sharing

- Voluntary disclosure between authorities; - No formal request requirement; Emergency situations

4. Joint Investigation Teams

- Multi-national task forces; - Coordinated operations; - Shared intelligence

5. 24/7 Point of Contact Network

- Emergency contact persons for each country; - Rapid international response capability; - Critical infrastructure protection

ADDITIONAL INTERNATIONAL FRAMEWORKS

African Union Convention on Cyberspace Security and Personal Data Protection (2014)

- Comprehensive African framework
- Data protection and cybersecurity
- Regional cooperation mechanisms
- Capacity building provisions

European Union Directive on Attacks Against Information Systems (2013)

- Establishes minimum cybercrime standards for EU member states
- Penalties and sanctions framework
- Critical infrastructure protection
- International cooperation mechanisms

UN General Assembly Resolutions on Cybersecurity

- Resolution 73/27 (2018): Advancement of responsible state behavior

- Resolution 54/51 (2000): General assembly calls on states to develop cyber law

- Focus on international norms, not binding treaties

International Telecommunications Union (ITU) Cybercrime Legislation Resources

- Toolkit for countries developing cyber law

- Best practices compilation

- Model legislation templates

Council of Europe Convention on Cybercrime Additional Protocol

- Addresses racist and xenophobic crimes online

- Criminal liability for hate speech propagation

- Enhanced penalties for bias-motivated cybercrimes

CYBER ETHICS AND DIGITAL MORALITY

Cyber Ethics is the branch of applied ethics dealing with moral principles and standards for responsible behavior in digital environments. It defines right and wrong conduct in online activities and cyberspace interactions.

Key Distinction from Cyber Etiquette (Netiquette):

- Cyber Ethics: Moral principles and values

- Cyber Etiquette (Netiquette): Rules of polite and respectful online conduct

SEVEN CORE PRINCIPLES OF CYBER ETHICS

1. Accountability

Responsibility for actions and decisions in digital environments.

Example: In financial system, audit logs prove specific employee unauthorized transfer; employee held legally accountable.

Organization Responsibility:

- Establish clear policies

- Provide user training

- Implement monitoring systems

- Enforce consequences for violations

2. Transparency

Openness in information sharing and communication practices.

Example: Social media platform clearly discloses data collection, usage, sharing practices to users before they sign up; explains algorithm factors determining feed visibility.

Benefits:

- Establishes trust

- Enables informed decision-making

- Facilitates accountability

- Supports regulatory compliance

3. Confidentiality

Protection of private information from unauthorized access or disclosure.

Scope: Personal data protection (names, contact info, financial data)

Mechanisms: Encryption of sensitive data

Violations and Consequences: Unauthorized disclosure of private information

Example: Hospital stores patient records with encryption; only authorized medical staff can access.

4. Integrity

Accuracy, completeness, and authenticity of digital information; absence of unauthorized modification.

Components: Data Integrity, System Integrity, Behavioral Integrity.

Protection Mechanisms:

- Cryptographic hash functions verifying file tampering

- Digital signatures proving document authenticity

Example: Digital forensics expert uses write-blocking device preserving hard drive integrity; maintains chain of custody documentation for admissibility in court.

5. Availability

Ensuring information and systems accessible to authorized users when needed.

Threats to Availability: Denial of Service attacks, Hardware failures

Protection Strategies: Redundant systems and backup, Load balancing across servers

Example: Bank implements geographic redundancy; if main data center fails, backup center automatically serves customers

6. Compliance

Adherence to applicable laws, regulations, industry standards, and ethical guidelines.

Regulatory Requirements: Data Protection: GDPR (EU), DPDP Act (India), CCPA (California)

Consequences of Non-Compliance:

- Financial penalties

- Legal prosecution

- Reputational damage

- Loss of business licenses or certifications

- Civil liability

7. Continuous Learning

Ongoing education and skill development to maintain ethical standards and address evolving threats.

Rationale:Technology landscape constantly changing, New threats and vulnerabilities emerge

Learning Mechanisms: Professional certifications (CISSP, CEH, CISM)

Organizational Programs: Annual cybersecurity awareness training

ETHICAL ISSUES IN CYBERSPACE

Issue	Ethical Concern	Example
Hacking	Unauthorized system access	Penetration testing without explicit written consent
Identity Theft	Impersonation and fraud	Using another person's social media profile
Plagiarism	Intellectual property violation	Copying content from website without attribution
Cyberbullying	Harassment and harm	Coordinated social media attacks on individual
Fake News	Misinformation spread	Publishing false political claims online
Privacy Invasion	Unauthorized surveillance	Recording private conversations without consent

CYBER ETIQUETTE (NETIQUETTE) GUIDELINES

Communication Standards:

1. Respect and Civility (Use polite language)

2. Clarity and Professionalism (Use clear, understandable language)

3. Relevance and Focus (Stay on topic in discussions)

4. Privacy Respect (Do not share others' private information)

5. Legal and Safe Behavior (Do not engage in illegal activities)

6. Acknowledgment and Credit (Cite sources and authors)

CHILD SEXUAL ABUSE MATERIAL (CSAM) IN CYBER DOMAIN

Child Sexual Abuse Material (CSAM) (also termed CSEM - Child Sexual Exploitation Material) is the recording, image, or video depicting the sexual abuse, exploitation, or coercion of a child or young person. It serves as documentation of child sexual abuse.

Indian Legal Definition (IT Act Section 67A/67B):

- Sexually explicit material featuring children (under 18 years)

- Computer-generated child sexual material

- Publishing, transmitting, possessing such material

CATEGORIES OF CSAM

A. Contact CSAM (Abuse-Generated)

- Origin: Direct sexual abuse of children

- Creator: Offender/abuser recording abuse

- Documentation: Evidence of real-time abuse

- Characteristics: Extreme trauma for victims

- Prevalence: ~30% of CSAM involves contact abuse

B. Self-Generated CSAM (SG-CSAM)

- Definition: Child creates sexually explicit images of themselves

Drivers:

- Consensual sharing among peers (youth sexting)
- Grooming by predator forcing self-imaging
- Extortion demanding image creation
- Live stream recording (streamed to predator)

C. Pseudo or Morphed CSAM

- Origin: Image created through digital manipulation
- Techniques:
  - Face-swapping onto nude bodies
  - Body parts editing
  - AI-generated synthetic CSAM
- Legal Status: Prosecutable in most jurisdictions despite no real abuse

D. Cartoon/Animation CSAM

- Depiction: Animated or drawn depictions of children in sexual acts

- Legality: Varies—prohibited in US, Canada, UK; legal in Japan

- Debate: Whether increases propensity for real abuse or provides outlet

E. Text-Based CSAM

- Content: Written descriptions of child sexual abuse

- Format: Stories, chats, forum posts

- Challenge: Difficult to prosecute;

ONLINE CSAM CHARACTERISTICS AND DISTRIBUTION

Production Methods:

1. Live Streaming: Real-time sexual abuse broadcast to paying subscribers (prevalence increasing)

2. Peer-to-Peer Networks: Direct file sharing between offenders, harder to trace

3. Darknet Markets: Encrypted networks enabling anonymous transactions

4. Social Media: Grooming and SG-CSAM solicitation through messaging

5. Cloud Storage: Upload to cloud services (Dropbox, Google Drive) for sharing

Offender Characteristics:

- Age Range: 13-70+ years (younger offenders involved in SG-CSAM)

- Motivation: Sexual gratification, financial gain, addiction

- Behavior Pattern: Escalation from viewing to contact abuse

- Organizational Level: Individual offenders to organized trafficking rings

Victim Impact:

- Immediate: Pain, trauma, fear, confusion

- Long-term: PTSD, depression, anxiety, suicide risk

- Re-victimization: Permanent online circulation of abuse images

- Cumulative Harm: Every share perpetuates original trauma

INDIAN LEGAL FRAMEWORK

IT Act Section 67A:

- Publishing images with sexual acts involving children

- Penalties: First offense: Up to 7 years and ₹10 lakh fine, Subsequent offense: Extended penalties

IT Act Section 67B:

- Possession of material depicting children in sexual acts

- Penalties: 3-8 years imprisonment and ₹5 lakh minimum fine

BNS Section 294A-294B:

- Obscene material broadly defined

Protection of Children from Sexual Offences Act (POCSO), 2012:

- Specialized law for child protection, - Recognizes SG-CSAM as abuse

- Acknowledges grooming as offense, - Victim protection measures

- Mandatory reporting requirements

Penalties for POCSO Violations:

Violation	Punishment
Aggravated penetrative sexual assault	10 years to life imprisonment
Sexual assault	3-5 years imprisonment
Child pornography	3-5 years imprisonment; 5-7 if aggravated

INVESTIGATION AND PROSECUTION CHALLENGES

Technical Challenges:

- Encryption: End-to-end encrypted platforms (WhatsApp) prevent content access

- Anonymity: Tor browser, VPNs enable perpetrator anonymity

- Darknet: Difficult to access and monitor illegal marketplaces

- Volume: Millions of images; resource constraints limit investigation

- File Verification: Determining if image real or synthetic

Legal Challenges:

- Jurisdiction: Cross-border offenses; unclear authority

- Extradition: Non-treaty countries refuse to extradite

- Chain of Custody: Digital evidence admissibility requirements strict

- Victim Identification: Necessary for contact abuse prosecution but privacy concerns

PREVENTION STRATEGIES

1. Technology-Based:

- Hash-matching preventing known CSAM distribution, - Content filtering on platforms

- Age verification systems, - Automated reporting tools

2. Education:

- School programs on online safety, - Parental monitoring guidance

- Child awareness of grooming tactics, - Professional training for educators and healthcare

3. Platform Responsibility:

- Prompt removal of reported material, - Grooming detection systems

- Cooperation with law enforcement, - Transparency reports on CSAM reports received/removed

RESPONSE PROTOCOLS

1. Immediate Reporting:

   - IIFC (Indian Internet Foundation) Council in India

   - National Center Exploitation of Children reporting

2. Victim Support:

   - Trauma counseling services, - Legal representation in proceedings

   - Confidentiality/anonymity protection, - Healing and recovery programs

3. Offender Prosecution:

   - Enhanced penalties for repeat offenders, - Sex offender registration

   - Containment and supervision, - Psychological treatment

ACTS AND LAWS RELATED TO SOCIAL MEDIA

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

Background:

Notified on February 25, 2021, these rules replace 2011 Intermediary Guidelines, establishing stricter compliance requirements for social media platforms, digital platforms, and search engines.

DEFINITION OF INTERMEDIARY

Any entity providing services including:

- Internet service providers

- Online marketplaces

- Social media platforms

- Messaging services

- Search engines

- Cloud computing services

- Content hosting platforms

A. GRIEVANCE REDRESSAL MECHANISM

Platforms must establish:

1. Designated Grievance Officer
   - Full-time employee in India
   - Responsibilities: Handle complaints, coordinate removal, maintain records
   - Contact information publicly available
2. Response Timelines
   - Acknowledgment: 24 hours of complaint
   - Resolution: 15 days for substantive response
   - Removal decision: 24-72 hours depending on content severity
3. Appeal Mechanism
   - Users can appeal removal decisions
   - Independent review process

B. CONTENT REMOVAL AND MODERATION

Platforms must:

1. Immediate Removal of content:

   - Threatening national integrity, sovereignty, security, - Inciting violence or hatred

   - Explicit sexual content involving minors, - Non-consensual intimate images, - Misinformation causing physical harm

2. Due Diligence:

   - Deploy technology tools detecting violative content, - Regular monitoring of platform

   - Proactive identification of violations, - Compliance with judicial orders

3. Prohibited Actions:

   - No hosting of obscene material, - No facilitating illegal activities

   - No enabling payment for prohibited services

C. USER VERIFICATION AND TRACEABILITY

1. Originator Identification:

   - Platforms must enable identification of original message/content creator

   - Only for law enforcement request with proper authorization

2. Non-Compliance Consequences:

   - Loss of safe harbor immunity

   - Criminal liability for platform's own actions

   - Civil penalties up to ₹1 crore per violation

D. TRANSPARENCY AND ACCOUNTABILITY

1. Quarterly Transparency Reports

   - Number of requests received from government

   - Number of content items removed

   - Breakdown of removal reasons

   - User account/suspension data

2. Privacy Policy Disclosures

   - Clear data collection practices

   - Data retention periods

   - Data sharing practices

   - User rights and choices

COMPREHENSIVE CHILD PROTECTION LAW WITH SPECIFIC SOCIAL MEDIA PROVISIONS (POCSO ACT 2012)

Offenses Related to Digital Platforms:

1. Online Grooming

   - Establishing sexual communication with child, - Intent to persuade into sexual act

   - Penalty: 5-10 years imprisonment and ₹1 lakh fine (minimum)

2. Solicitation of Child Sexual Material

   - Requesting, seeking images from minor, - Inducing child to create/transmit material

   - Penalty: 3-8 years imprisonment and ₹5 lakh fine

3. Fabricated Material

   - Creating fake explicit images of child, - Morphing real images into explicit form

   - Penalty: 3-8 years imprisonment

4. Distribution and Transmission

   - Forwarding CSAM received, - Live streaming child sexual abuse

   - Penalty: 3-8 years imprisonment and ₹5 lakh fine (minimum)

SPECIAL PROVISIONS

- Child treated as victim, not criminal offender (even for SG-CSAM)
- Gender-neutral protections
- In-camera trials protecting child identity
- Witness protection programs
- Free legal aid for victims

DEFAMATION AND PRIVACY LAWS IN SOCIAL MEDIA CONTEXT

DEFAMATION (Section 356 BNS)

Section 356(1) of the BNS defines defamation as making or publishing any imputation concerning another person through words (spoken or written), signs, or visible representations with the intention to harm, or knowing or having reason to believe that such imputation will harm, the reputation of that person.

Key Elements: False Statement, Harm to Reputation, Publication, Intent or Knowledge

Under Section 356(2), whoever defames another shall be punished with

Simple imprisonment for a term which may extend to two years, OR Fine, OR Both, OR Community service

SEXUAL HARASSMENT (Section 75 BNS)

Section 75(1) of the BNS defines sexual harassment as a man committing any of the following acts:

(i) Physical contact and advances involving unwelcome and explicit sexual overtures

(ii) A demand or request for sexual favours

(iii) Showing pornography against the will of a woman

(iv) Making sexually coloured remarks Punishment

The punishment varies based on the nature of the offence

For acts under clauses (i), (ii), or (iii) Rigorous imprisonment for a term which may extend to three years, OR Fine, OR Both

For acts under clause (iv) Imprisonment of either description for a term which may extend to one year, OR Fine, OR Both

CRIMINAL INTIMIDATION (Section 351 BNS)

Section 351(1) defines criminal intimidation as threatening another person by any means with any injury to:

The person, reputation, or property, OR The person or reputation of anyone in whom that person is interested

With the intent to: Cause alarm to that person, OR Cause that person to do any act which they are not legally bound to do, OR Omit to do any act which they are legally entitled to do

Explanation: A threat to injure the reputation of any deceased person in whom the person threatened is interested falls within this section

Basic Criminal Intimidation [Section 351(2)]:

Imprisonment of either description for a term which may extend to two years, OR Fine, OR Both

Aggravated Criminal Intimidation [Section 351(3)] — threatening to cause:

Death or grievous hurt; Destruction of property by fire; An offence punishable with death or life imprisonment or imprisonment up to seven years; Imputing unchastity to a woman

Punishment:

Imprisonment of either description for a term which may extend to seven years, OR Fine, OR Both

Anonymous Intimidation [Section 351(4)] — by anonymous communication or concealing the sender's identity: Imprisonment of either description for a term which may extend to two years, in addition to the punishment under Section 351(1)

OUTRAGE OF MODESTY

Section 74 BNS: Assault or Criminal Force to Woman with Intent to Outrage Her Modesty

Section 74 criminalizes assault or use of criminal force against any woman with the

intention of outraging, or knowing it to be likely that it will outrage, her modesty.

Key Elements:

Assault or use of criminal force against a woman

Intent to outrage her modesty, OR

Knowledge that such action is likely to outrage her modesty

Punishment

Imprisonment of either description for a term which shall not be less than one year but which may extend to five years, AND Fine (mandatory)

Section 76 BNS: Assault or Use of Criminal Force to Woman with Intent to Disrobe

Section 76 specifically addresses the more serious offence of assaulting or using criminal force against any woman, or abetting such act, with the intention of disrobing or compelling her to be naked

Punishment

Imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, AND Fine (mandatory)

Distinction from Section 74

Section 76 is a more specific and aggravated form of outraging modesty. While Section 74 covers general acts of assault with intent to outrage modesty, Section 76 specifically targets acts aimed at forcibly removing a woman's clothing or making her naked

Section 79 BNS: Word, Gesture or Act Intended to Insult the Modesty of a Woman

Section 79 criminalizes acts where a person, intending to insult the modesty of any woman:

Utters any words, makes any sound or gesture,

or Exhibits any object in any form, intending that such word, sound, gesture, or object shall be heard or seen by the woman,

or Intrudes upon the privacy of such woman

Punishment Simple imprisonment for a term which may extend to three years, AND Fine

PRIVACY AND SECURITY IN CYBER DOMAIN

Constitutional Foundation (India):

Article 21 - Right to Life and Personal Liberty

- Interpreted to include right to privacy

Right to Privacy Components:

1. Informational Privacy: Control over personal data

2. Decisional Privacy: Freedom from government interference in choices

3. Bodily Privacy: Protection from physical intrusion

DATA PROTECTION LAWS

Digital Personal Data Protection Act, 2023 (DPDP Act)

Replacing Earlier Framework:

- Sensitive Personal Data and Information (SPDI) Rules 2011, - Partial implementation of IT Act provisions

- A. Applicability and Scope

- Applies to processing of digital personal data within India

- Extraterritorial application: Data of Indian residents processed abroad

- Does NOT apply to:

  - Non-digital personal data

  - Non-personally identifiable information

  - Government processing (different framework)

B. Core Definitions

Data Principal: Individual to whom personal data relates; equivalent to GDPR (General Data Protection Regulations) "data subject"

Data Fiduciary: Entity determining purpose and means of data processing; equivalent to GDPR "controller"

Data Processor: Entity processing data on fiduciary's behalf; equivalent to GDPR "processor"

Digital Personal Data: Information in digital form about identifiable individual

C. Core Principles of Data Processing

1. Lawfulness and Fairness (Processing must have legal basis)

2. Purpose Limitation (Processing limited to stated purpose)

3. Data Minimization (Collect only necessary data)

4. Accuracy and Quality (Data kept accurate and up-to-date)

5. Storage Limitation (Data retained no longer than necessary)

6. Integrity and Confidentiality (Security measures protecting data)

7. Accountability (Responsibility for data handling)

D. Rights of Data Principals

1. Right to Information (Notice before data collection)

2. Right to Access (Obtain copy of personal data held)

3. Right to Correction (Correct inaccurate data)

4. Right to Erasure (Delete data under circumstances:- No longer needed for purpose, - Consent withdrawn, - Unlawful processing, - Exceptions for legal compliance)

5. Right to Data Portability (Receive data in portable format)

6. Right to Grievance Redressal (Submit complaints to Data Protection Board)

E. Children's Data Protection

1. Verifiable Parental Consent

   - Must obtain parental consent for under-18 processing, - Verified parental identity confirmed

   - Age verification mechanisms

2. Restricted Processing for Children

   - Prohibited for targeted advertising, - Prohibited for profiling

   - Limited to service delivery and safety

3. Specific Safeguards

   - Higher transparency requirements, - Clear language in notices

   - Additional oversight mechanisms

F. Significant Data Fiduciaries

Entities with large-scale data processing designated as "Significant Data Fiduciaries" (SDFs):

Obligations:

- Appoint Data Protection Officer (DPO) in India
- Conduct Data Protection Impact Assessment (DPIA)
- Regular audits and assessments
- Enhanced transparency measures
- Stricter compliance requirements

Thresholds:

- Processing data of 1 million individuals
- Significant volume of sensitive data
- Data processing with high risk

G. Data Protection Board of India

Independent regulatory authority:

Functions:

- Investigate complaints, - Issue compliance orders, - Impose penalties for violations

- Hear appeals, - Issue guidelines

Violation	Penalty
Non-compliance with notice	Up to ₹50 lakh
Unauthorized processing	Up to ₹500 crore
Failure to implement safeguards	Up to ₹500 crore
Data breach without notification	Up to ₹500 crore

CYBERSECURITY STANDARDS AND FRAMEWORKS

NIST Cybersecurity Framework (US)

Five Core Functions:

1. Identify(-Asset inventory, - Risk assessment, - Business continuity planning, - Threat intelligence)

2. Protect (- Access controls, - Encryption, - Vulnerability management, - Security training)

3. Detect (- Continuous monitoring, - Intrusion detection systems, - Security information and event management (SIEM), - Anomaly detection)

4. Respond (- Incident response plans, - Communication procedures, - Investigation protocols, - Eradication and recovery)

5. Recover (- Business continuity plans, - Disaster recovery procedures, - System restoration, - Post-incident analysis)

ISO/IEC 27001 - Information Security Management

International standard for information security management systems:

- Risk assessment and treatment
- Asset management
- Access control
- Cryptography implementation
- Physical and environmental security
- Incident management
- Business continuity
- Compliance management