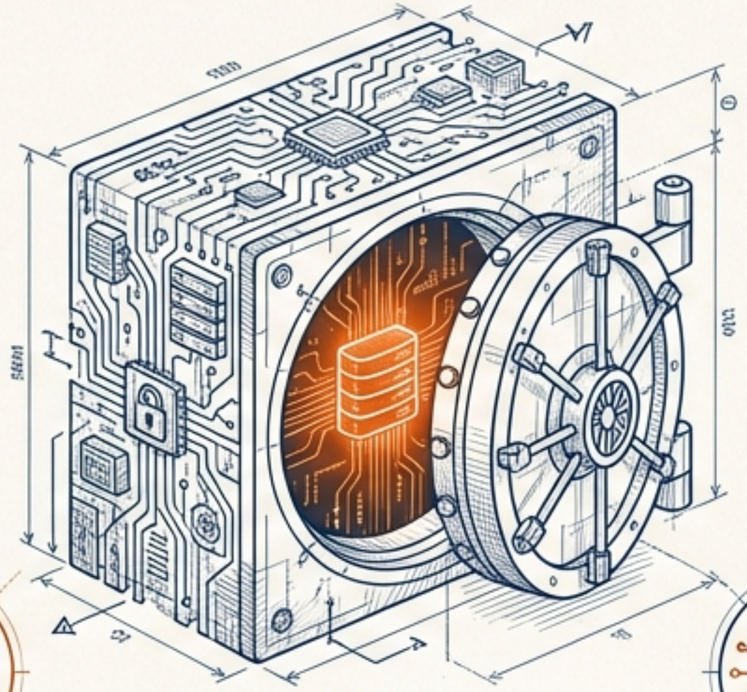
सूचना का किला: इनफार्मेशन सिक्योरिटी के मूल सिद्धांत

IT Systems - Unit 5 (One Shot Revision)



1. सुरक्षा की नींव

InfoSec vs. CyberSec

2. डिजिटल दुश्मन

Threats & Malware

3. सुरक्षा कवच

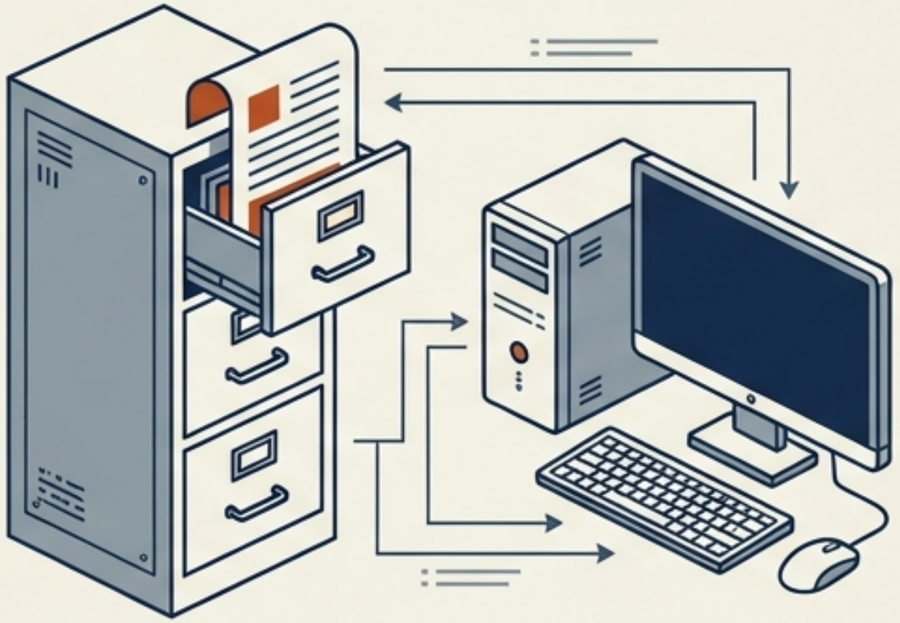
Cryptography, Firewall, IDS/IPS

4. भारत का कानून

IT Act 2000 & DPDP 2023

सुचना सुरक्षा (InfoSec) बनाम साइबर सुरक्षा (CyberSec)

Information Security (InfoSec)



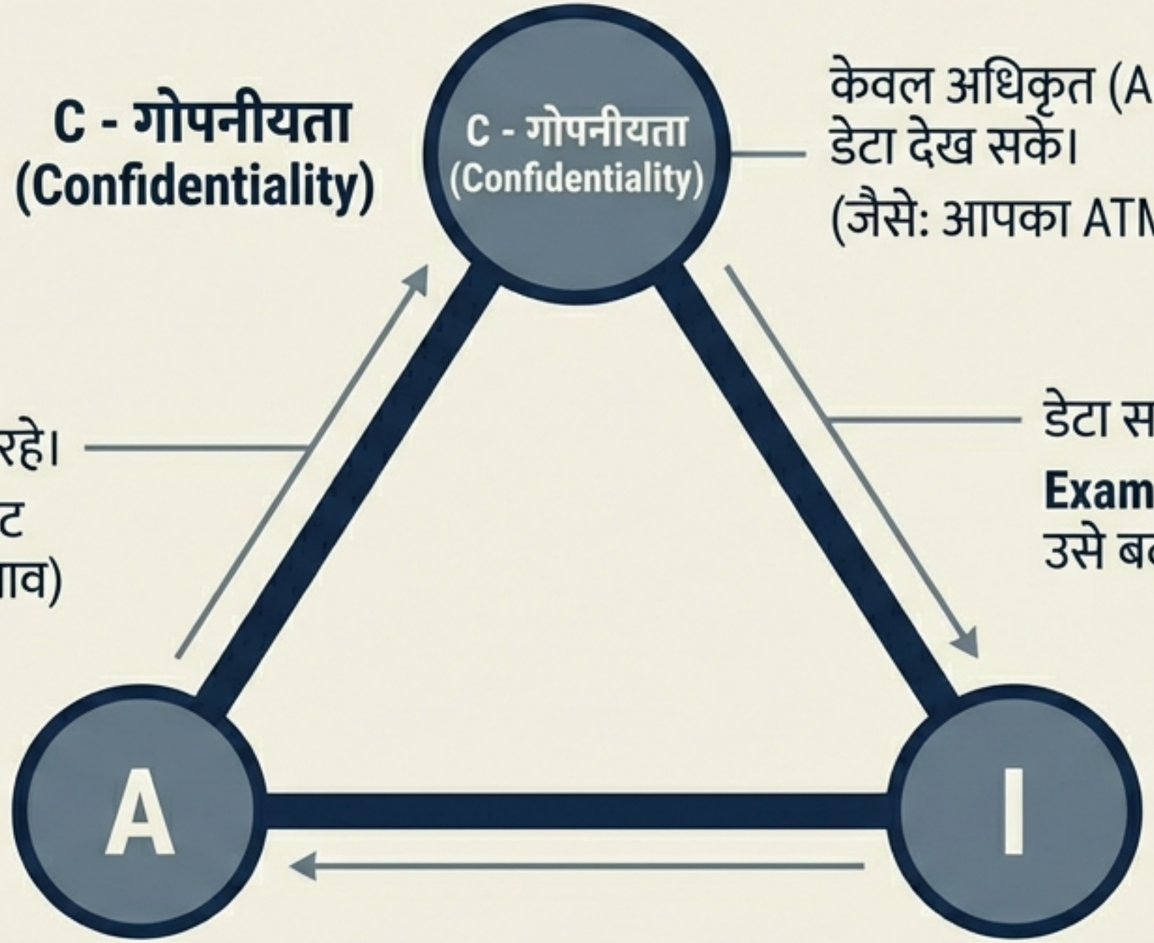
- यह डिजिटल और गैर-डिजिटल (कागजी) दोनों प्रकार के डेटा की सुरक्षा है।
- **Example:** कंपनी की फाइलों (Paper Files) की चोरी या सर्वर हैक होना।

Cyber Security

- यह केवल डिजिटल डेटा (नेटवर्क, कंप्यूटर, सर्वर) की सुरक्षा है।
- **Example:** Facebook या Bank Server का हैक होना।

Key Insight: साइबर सुरक्षा, इनफार्मेशन सिक्योरिटी का ही एक हिस्सा है।

सुरक्षा का त्रिकोण: The CIA Triad



सुरक्षा क्यों जरूरी है? (Need for Security)

व्यक्तिगत (Personal)

निजी फोटो, बैंक डिटेल्स और Identity Theft से बचाव।

व्यावसायिक (Business)

ग्राहकों का भरोसा और वित्तीय नुकसान (Financial Loss)।

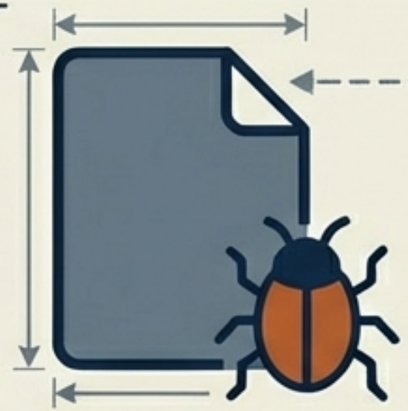
यदि Facebook का डेटा लीक हुआ, तो यूजर भरोसा करना बंद कर देंगे।

राष्ट्रीय सुरक्षा (National Security)

सरकारी संस्थान और रक्षा डेटा।

Critical Example: RAW एजेंट्स की जानकारी लीक होने से देश की सुरक्षा और सैनिकों की जान को खतरा हो सकता है।

मैलवेयर: डिजिटल दुनिया के कीड़े (Malware Types)

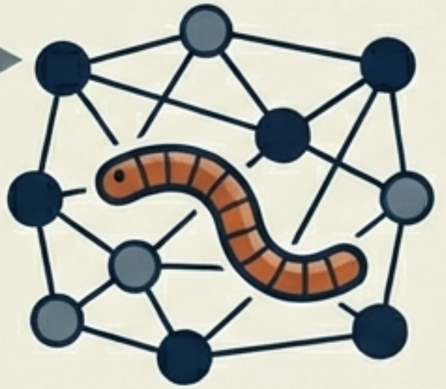


Virus (वायरस)

फाइलों से चिपक कर आता है (.exe), यूजर के क्लिक करने पर फैलता है।

Worms (वॉर्म्स)

यह नेटवर्क के जरिए खुद फैलता है (Self-replicating), इसे यूजर की गलती की जरूरत नहीं होती।



Trojan Horse (ट्रोजन)

यह वैध सॉफ्टवेयर जैसा दिखता है लेकिन पीछे से नुकसान पहुंचाता है।

Example: 'Fake YouTube App' जो असली जैसा दिखता है पर डेटा चोरी करता है।

Ransomware (रैंसमवेयर)

डेटा को एन्क्रिप्ट (Lock) करके फिरौती (Money) मांगता है।

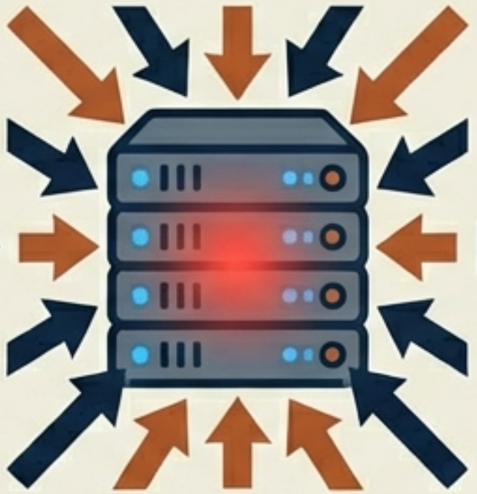
Money (फिरौती)

नेटवर्क और वेब पर होने वाले हमले (Network Threats)

Phishing (फिशिंग)

फर्जी ईमेल या वेबसाइट के जरिए पासवर्ड चुराना (जैसे: Flipkart की नकली लिंक)।

DDoS (Denial of Service)



सर्वर पर इतना ट्रैफिक भेजना कि वह 'Busy' हो जाए और असली यूजर एक्सेस न कर पाए।

SQL Injection

डेटाबेस में malicious code डालकर डेटा चोरी करना।

Man-in-the-Middle (MitM)

दो लोगों के कम्युनिकेक्शन के बीच में छिपकर बातें सुनना।

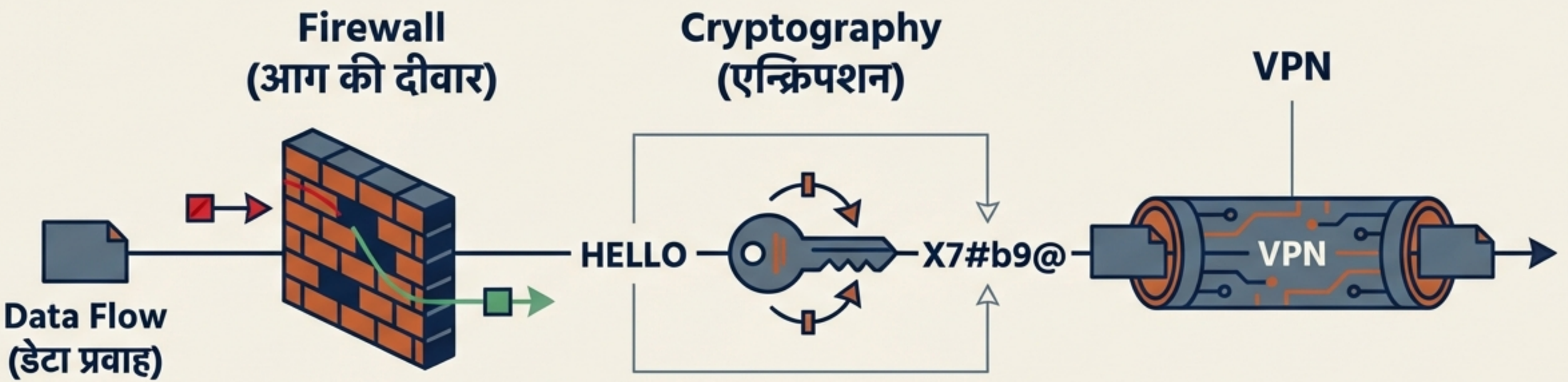
भौतिक और मानवीय खतरे (Physical & Human Threats)

- **भौतिक खतरे (Physical Threats):** आग, पानी, या बिजली (Short Circuit) से हार्डवेयर का नुकसान। लैपटॉप या हार्ड ड्राइव की चोरी।
- **इनसाइडर थेट्स (Insider Threats):** कंपनी का ही कोई कर्मचारी जो एक्सेस का दुरुपयोग करे।
- **सोशल इंजीनियरिंग (Social Engineering):** इंसान को बेवकूफ बनाकर पासवर्ड मांगना (जैसे: 'सर, मैं बैंक से बोल रहा हूँ, OTP बताइये')।
- **Identity Theft:** किसी और की पहचान (आधार/पैन) का उपयोग करके फ्रॉड करना।

व्यक्तिगत सुरक्षा: आपकी पहली जिम्मेदारी (Best Practices)

- [x] **मजबूत पासवर्ड (Strong Password)**
  कम से कम 12 अक्षर. Number, Symbol, Capital & Small letters.
  ✗ Bad: Vikas@123 ✓ Good: #Vi$23@Mn
- [x] **2FA (Two-Factor Authentication)**
  पासवर्ड के बाद OTP या बायोमेट्रिक अनिवार्य करें।
- [x] **नियमित अपडेट (Regular Updates)**
  सॉफ्टवेयर और एंटीवायरस को हमेशा अपडेट रखें।
- [x] **सतर्कता (Vigilance)**
  किसी भी अनजान लिंक (Suspicious Link) पर क्लिक न करें।

तकनीकी सुरक्षा कवच (Technical Defense)



यह नेटवर्क ट्रैफिक को फिल्टर करता है। अनचाहे ट्रैफिक को रोकता है।

डेटा को 'कोड' भाषा में बदलना।
Example: WhatsApp End-to-End Encryption.

पब्लिक नेटवर्क पर सुरक्षित और एन्क्रिप्टेड कनेक्शन।

निगरानी तंत्र: IDS बनाम IPS

IDS
(Intrusion Detection System)

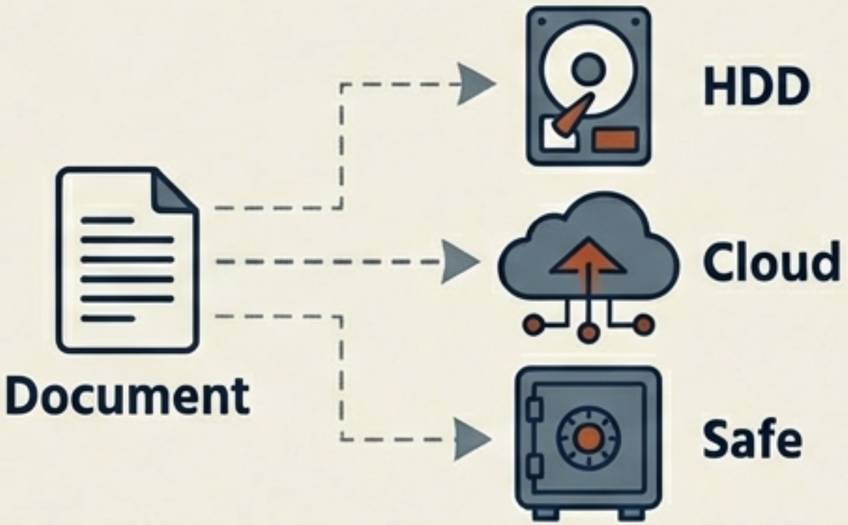
- यह घुसपैठ की **पहचान** करता है।
- सिर्फ **Alert** भेजता है (जैसे CCTV)।
- हमले को रोकता नहीं है।

IPS
(Intrusion Prevention System)

- यह घुसपैठ को **रोकता** है।
- संदिग्ध ट्रैफिक को **Block** कर देता है।

Exam Tip: IDS सिर्फ देखता है, IPS कार्रवाई करता है।

बैकअप और वायरलेस सुरक्षा (Backup & Wireless)



डेटा बैकअप (Data Backup)

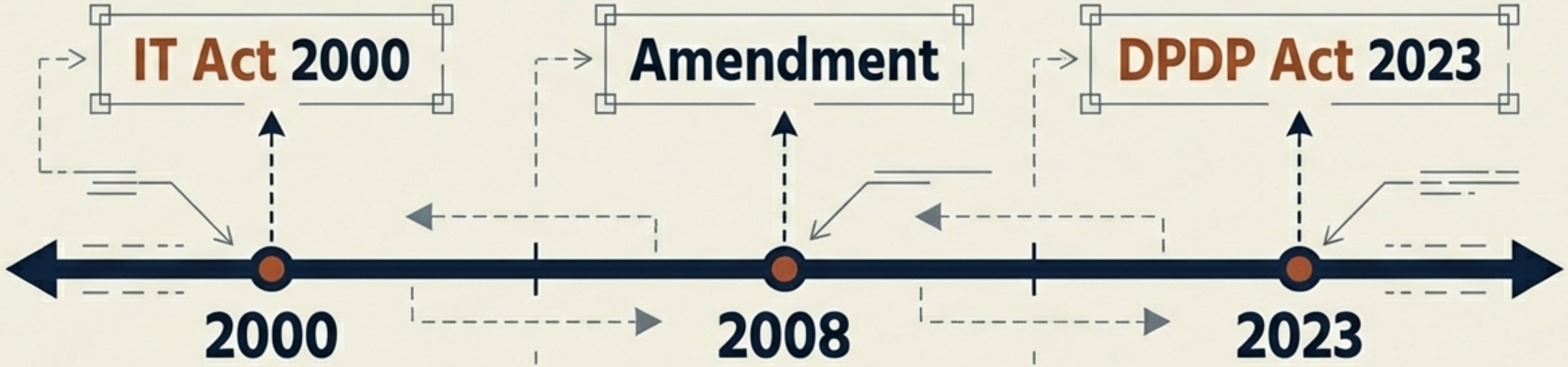
3-2-1 Backup Rule: नियमित रूप से डेटा की कॉपी बनाएं।

Tools: HDD, Google Drive.

वायरलेस सुरक्षा (Wi-Fi Security)

- हमेशा **WPA2** या **WPA3** एन्क्रिप्शन का उपयोग करें।
- SSID Broadcast को Disable रखें।
- ओपन/पब्लिक वाई-फाई पर बैंकिंग न करें।

भारतीय साइबर कानून (Indian Cyber Law Framework)



- भारत का प्राथमिक कानून जो साइबर अपराध और **ई-कॉमर्स** को नियंत्रित करता है।

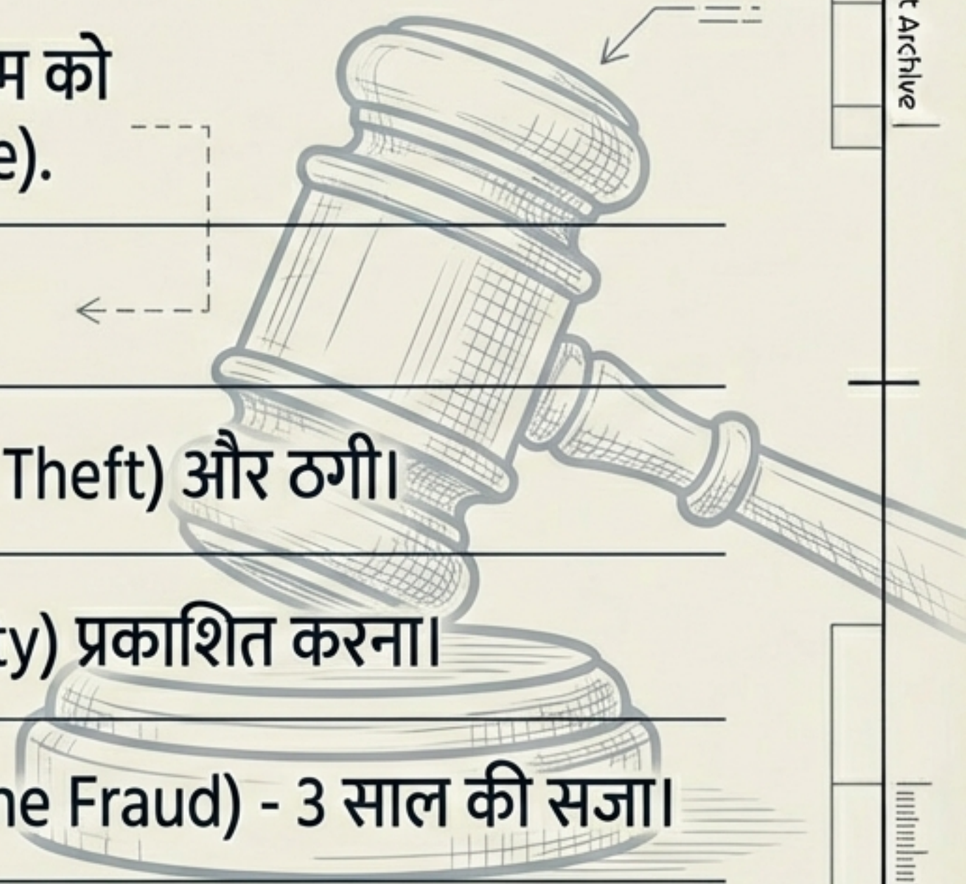
Section 66A (हटाया गया) और **Section 69** (National Security) जोड़े गए।

Digital Personal Data Protection.

- यूजर की सहमति (Consent) अनिवार्य।
- डेटा लोकलाइजेशन (Data Localization)।

प्रमुख धाराएं और सजा (Key Sections & Penalties)

Section 43	बिना अनुमति कंप्यूटर सिस्टम को नुकसान पहुंचाना (Damage).
Section 66 (Hacking)	**3 साल की जेल** + जुर्माना।
Section 66C & 66D	पहचान की चोरी (Identity Theft) और ठगी।
Section 67	अश्लील सामग्री (Obscenity) प्रकाशित करना।
Section 420	ऑनलाइन धोखाधड़ी (Online Fraud) - 3 साल की सजा।



निगरानी और सुरक्षा एजेंसियां (Agencies & Surveillance)

Government of India

Section 69 (Power)

राष्ट्रीय सुरक्षा के लिए डेटा इंटरसेप्शन और डिक्रिप्शन की शक्ति।

CERT-In

Emergency Response. साइबर हमालों के दौरान बचाव कार्य।

NCIIPC

Critical Infrastructure Protection (Power grids, Defense).

DPDP 2023 Penalty: डेटा सुरक्षा नियमों का उल्लंघन करने पर कंपनियों पर **500 करोड़** तक का जुर्माना।

परीक्षा के लिए महत्वपूर्ण बिंदु (Summary & Exam Focus)

Note to Self

- **CIA Triad:** गोपनीयता (Confidentiality), अखंडता (Integrity), उपलब्धता (Availability)।
- **Differences:** InfoSec vs CyberSec और IDS vs IPS को स्पष्ट याद रखें।
- **Law:** IT Act 2000 और Section 66 (हैकिंग - **3 साल सजा**)।
- **Security is a Process:** सुरक्षा कोई प्रोडक्ट नहीं, निरंतर प्रक्रिया है।

"सतर्क रहें, सुरक्षित रहें (Be Alert, Be Safe)."