CYBER LAW: PROTECTING RIGHTS IN THE DIGITAL AGE

Presented by: Mr. Upender Thakur, Advocate

CYBER LAW

Law of the Internet or IT laws, being a legal system designed to deal with the internet, computing, cyberspace, and related legal issues, is faced with many challenges in this age of Generative AI, Algorithmic decision making, Digital Identity, Digital Evidence etc.

From coming in to force to give legal recognition/validity/sanctity to electronic documents/commerce, digital signature, transactions carried out by means of electronic data interchange and other means of electronic communication, the canopy of cyber law has expanded into many amendments, enactments, rules and framework addressing data protection, cyber security and intermediary accountability, which encompass as following:

- **The Information Technology Act, 2000**: Establishes the legal framework for electronic governance, defining offences like hacking (Section 66), publishing obscene material (Section 67), and ensuring extraterritorial jurisdiction (Section 75) for cybercrimes involving systems in India.
- **The Information Technology (Amendment) Act, 2008**: Strengthens cybersecurity with provisions addressing identity theft (Section 66C), cheating via impersonation (Section 66D), lawful interception of communication (Section 69), and protection of critical infrastructure (Section 70).
- **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2011**: Requires intermediaries to inter-alia, moderate content, ensure traceability, and remove unlawful material within 36 hours of notification while protecting user data.
- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, 2011:** Establishes mandatory guidelines for organizations to implement reasonable security practices, inter-alia, protecting sensitive personal data from unauthorized access, defining security obligations, and providing recourse in case of data breaches.
- **The Finance Act, 2017**: Inter-alia, expanded the jurisdiction of the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) to include matters previously under the Cyber Appellate Tribunal, consolidating appellate functions related to cyber disputes.
- **The Jan Vishwas (Amendment of Provisions) Act, 2023**: Inter-alia, decriminalizes minor cyber offences to simplify compliance, promoting ease of doing business and streamlining penalties in cyber-related laws.
- **The Digital Personal Data Protection Act, 2023**: Regulates inter-alia data processing activities, ensures privacy, and enforces obligations on organizations to secure personal data while addressing cybersecurity risks.
- **Bhartiya Nyaya Sanhita, 2023**

THE DIGITAL AGE

The digital age reflects a scenario of digitally connected environment driven by computers, computer network, computer resource, communication device etc. in the conspectus of the age of instant dissemination through digital technology and internet. The rise of social media, smartphones and digital platforms has given a new dimension to medium of expression and communication. The growth of OTT platforms, 4G/5G connectivity, digital payments and online services further integrated technology into everyday life, while creating new concerns relating to data protection, cybercrime, online safety and consumer rights. Today, with the emergence of Artificial Intelligence, algorithms and deepfakes, technology is influencing not only communication but also identity, decision-making and access to information. Thus, the digital age while adding many facets, has brought numerous challenges so far as rights, also metamorphosing in to digital rights now, are concerned ;

- **Artificial Intelligence (AI)**

- AI refers to the simulation of human intelligence in machines, enabling them to perform tasks like decision-making, pattern recognition, and problem-solving.

- **Cybersecurity Threats:**

- **Deepfakes and Misinformation:** AI can be used to create convincing fake images, videos, and news, leading to social and political harm.
- **AI-powered Attacks:** Hackers use AI to automate and enhance phishing, brute force attacks, and malware creation.
- **Bias and Discrimination:** Unregulated AI systems may perpetuate biases, leading to ethical and legal disputes.
- **Autonomous Systems:** AI-driven devices or systems (e.g., drones, self-driving cars) may malfunction or be hijacked, raising concerns about liability and accountability.

PROTECTION OF RIGHTS IN DIGITAL AGE

➢ **<u>Understanding scope and applicability of IT Act 2000</u>**

❖ In **Yes Bank Limited Vs Wardha Nagari Sahakari Adhikosh (Bank) & Ors**., the Hon'ble TDSAT Vide Judgement dated 29.05.2026 in re: CA No. 3 of 2025, inter alia, has passed general directions in terms of section 57 (4) read with section 58 (1) of the IT Act 2000 to adjudicating officers functioning under section 46 of IT Act, across all states & UTs to unify and streamline the procedure to ensure ***access to justice*** in the light of mandatory requirements of article 14, 21 and 39 A of the Constitution of India, 1950.

❖ The Hon'ble TDSAT with the passing of the above mentioned general direction, has held in no uncertain terms that section 46(2) of IT Act read with rule 4 (c), 4(d), 4(h), 4(j) and 7 of the information Technology (Qualification & Experience of Adjudicating officers & manner of holding inquiry) Rules, 2003 lays down for ***reasonable and effective opportunity of hearing***. While laying emphasis on the principles of audi alteram partem requiring inquiry as well as representation, the Hon'ble TDSAT has opined that the unilateral disposal of the complaint by Adjudicating officer is not permissible at all.

❖ The Hon'ble TDSAT discussing in detail the salient provisions of IT Act, has also held that section 62 carving out remedy of appeal to Hon'ble High Court on any question of fact or law, recognises that disputes under IT Act may involve technically complex question of fact relating to cyber security, forensic evidence, digital forensics, IP address analysis & system vulnerabilities which may require independent judicial examination even at the second appellate stage, the same therefore necessitating & warranting reasonable & effective opportunity of hearing at the very first stage of complaint before Adjudicating officer under IT Act.

❖ The Hon'ble TDSAT while observing that ''speed may shorten time, it can not abrogate fairness and due process", has clearly laid emphasis on dovetailing the interest & rights of all stake holders on the anvil of principles of natural justice and fair play.

Threats In Digital Age

AWARENESS OF CYBER CONTRAVENTIONS AND OFFENCES IS ALSO A WAY TO UNDERSTAND ABOUT RIGHTS AND REMEDIES.

Fraudulent Electronic Fund Transfers:

- Unauthorized electronic fund transfers, often achieved via phishing, malware, or fraudulent OTPs.
- Culpability and Liability:

  Section 43 and section 43A of IT Act, 2000: Civil liability to pay damages by way of compensation.

  Section 66 of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹5,00,000.

- In **Bank of India v. Sri Sandeep**, The Hon'ble TDSAT vide judgment dated 20.12.2019 in re: Cyber Appeal 3 of 2018 held the bank liable under Section **43A** of the IT Act, 2000, in the facts of the case, for failing to implement reasonable security practices, leading to unauthorized transactions and also held the Telecom Service Provider liable under sections **43A** and **43(g)** of IT Act, 2000. The Hon'ble Tribunal held that there is a contributory negligence on part of the bank and the Telecom Service Provider paving the way for siphoning off money from the victim's account.

This Judgement holding untrammelled sway, is continuing to be applied from time to time in various cases involving the same factual matrix and legal score.

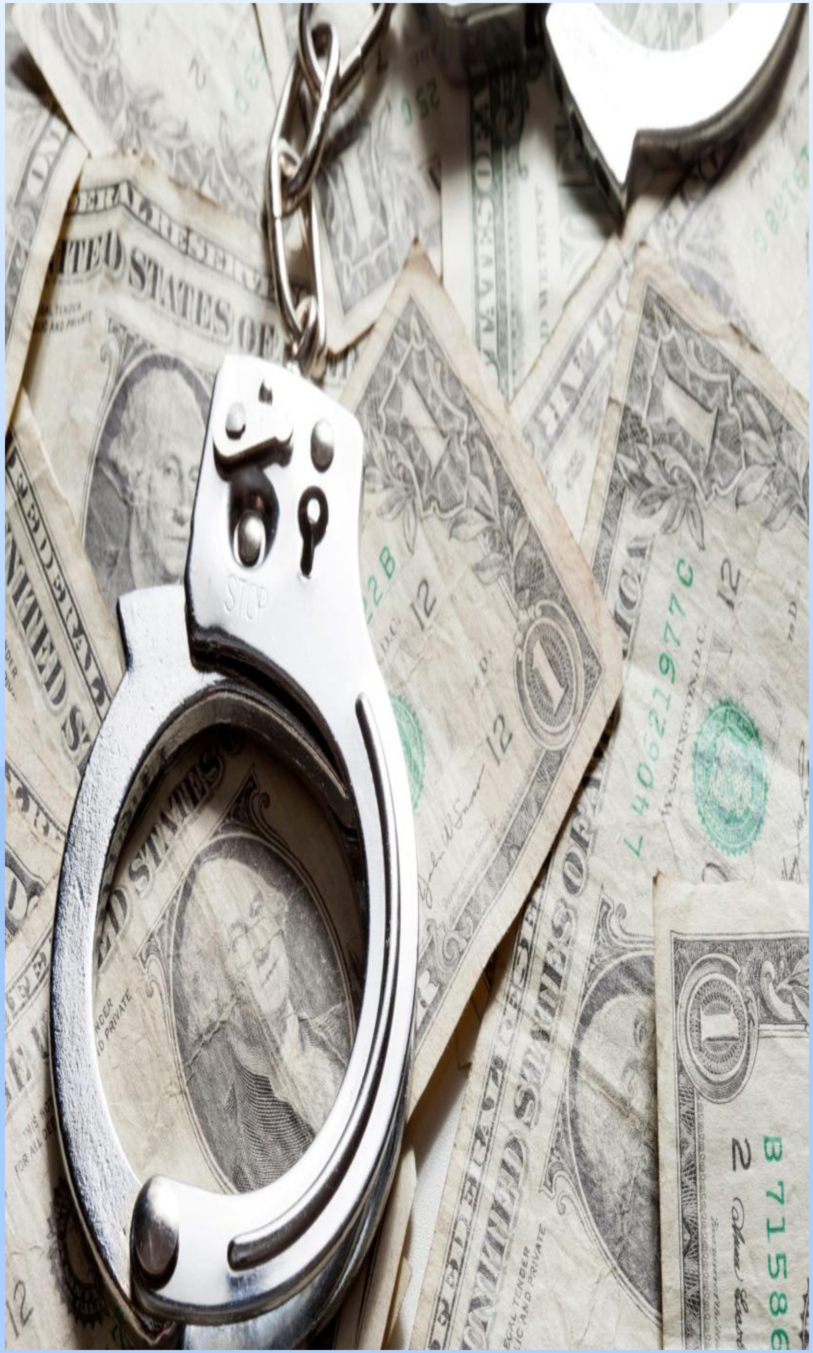
- **<u>Mule Accounts</u>**: Bank accounts that facilitate illegal transactions by receiving and transferring funds from unlawful activities, with or without the complicity of the account holders.
- Culpability and Liability:
    - Section 66D: Imprisonment up to 3 years and fine up to ₹1,00,000.
    - IT Act, 2000: Section 43(a) (unauthorized access) and Section 66D (cheating by impersonation).
    - **RBI master circular dated 2 July 2012 issued to banks as per PMLA,2002 lays down precautions to be taken qua money mule accounts(refer para 2.8 thereof)**

- **<u>ATM Skimming or Card Cloning:</u>** Stealing card information using skimmers or creating cloned cards to withdraw money.
- Culpability and Liability: Section 66C of IT Act, 2000: Imprisonment up to 3 years and fine up to ₹1,00,000.

- In **Manvir Singh Vs ICICI Bank**, the Hon'ble TDSAT vide judgment dated **04.08.2026** in re : **Cyber Appeal 10** of **2020** gave wider connotation to "**reasonable security practice**" under section **43 A of IT Act, 2000**.

The Hon'ble TDSAT held the bank to be liable under payment & Settlement System Act, 2007 (RBI Circular dated **28.02.2013** issued under **section 18** of the Act to all scheduled Commercial Banks/ Urban Cooperative Banks / State Cooperative Banks, District Central Co-operative Banks thereby, directing guidelines on security card transaction and securing electronic payment transections), **RBI Circular dated 24.09.2011** being guidelines on information, security, electronic banking, technology risk management and cyber frauds, with detailed instructions to all banks on fraud risk management, KYC Norms, transection monitory, dedicated email ID and phone No. of reporting suspected frauds, mystery shopping and refuse, reporting of fraud, filing of police complaint by bank in case of fraud against there customer, customer awareness etc., **RBI Circular dated 2.7.2012** about KYC norms/ anti money laundering standards/ combating of financial terrorism under **Public Money Laundering Money Act, 2002.**

While placing reliance on Judgment In re: **CA No. 5 of 2018,** The Hon'ble TDSAT observed that compliance of sending SMS alert by registering mobile No. as well as email ID is mandatory for banks, for maintaining its reasonable security practice in internet banking.

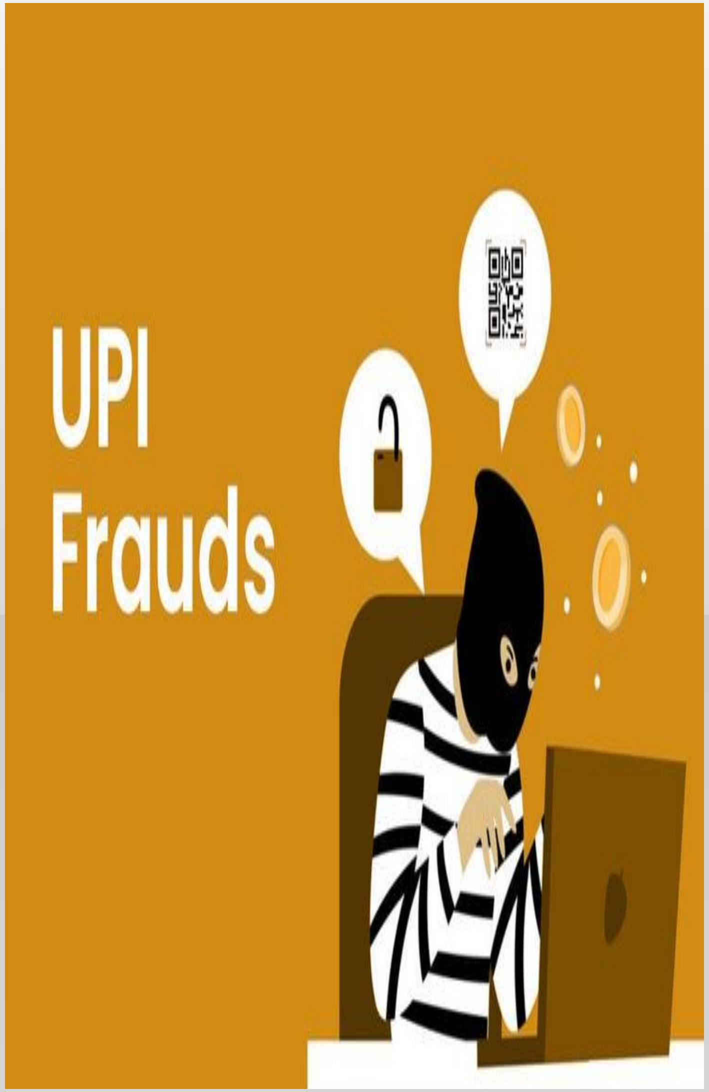


<u>UPI Payment Frauds</u>: Unauthorized transactions carried out using a victim's UPI account, often by tricking them into sharing sensitive information such as UPI PINs or OTPs, or through malicious apps.

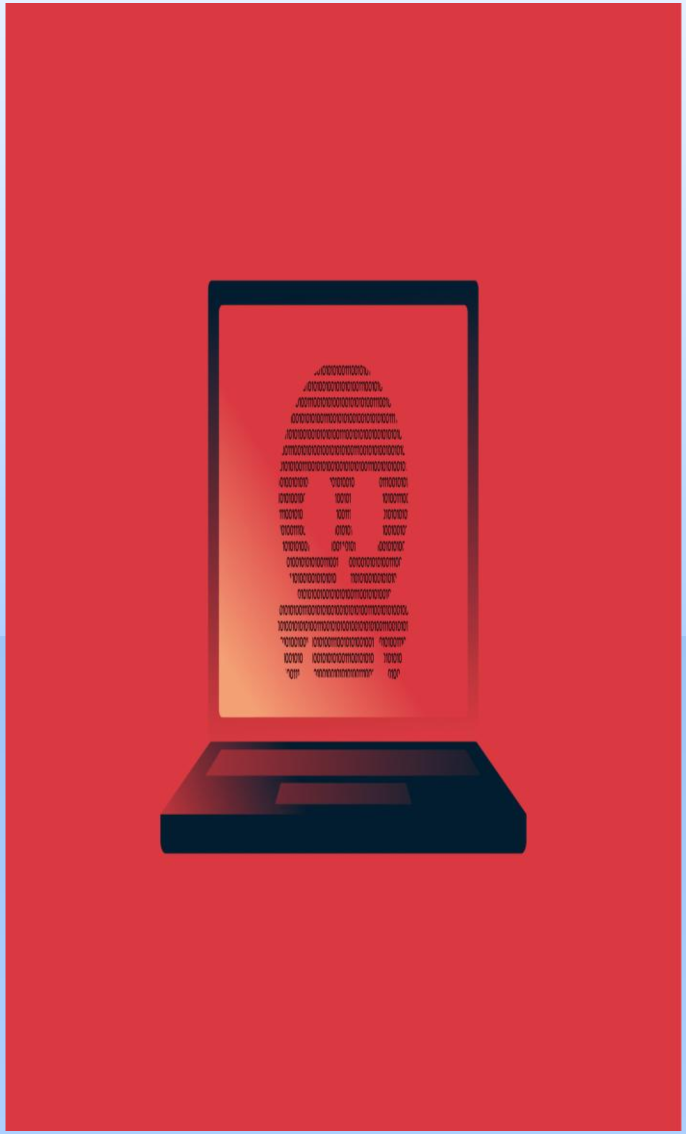
Culpability and Liability: Section 43 and section 43A of IT Act, 2000: Civil liability to pay damages by way of compensation **and/or Section 66 of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹5,00,000.**

. <u>OTP-Based Frauds</u>: Frauds where either victims are deceived into sharing One-Time Passwords (OTPs) sent to their registered mobile numbers or *otherwise*, enabling unauthorized access to their bank or payment accounts.

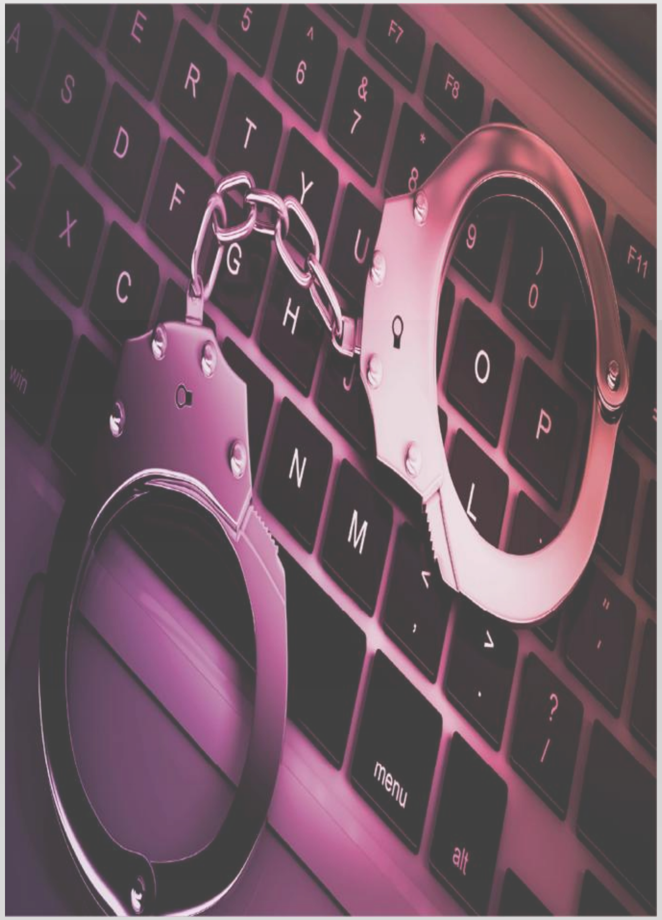
Culpability and Liability: Section 43 and section 43A of IT Act, 2000: Civil liability to compensate the victim and/or Section 66 of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹5,00,000.



- **<u>Cyber Extortion</u>: Threatening to harm or reveal sensitive digital information unless a ransom is paid. A new form of extortion by the name, <u>Sextortion</u>, is also on the rise nowadays, which means blackmailing someone by threatening to release explicit content unless demands are met.**
- **Culpability and Liability: Section 66E of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹2,00,000 and/or Section 67 of IT Act, 2000: Imprisonment up to 5 years and fine up to ₹10,00,000 and/or Section 67A of IT Act, 2000: Imprisonment up to 7 years and fine up to ₹10,00,000.**
- **<u>Cyber arrest</u>:** It occurs when individuals are wrongfully detained by imposters posing as law enforcement or cybercrime authorities. These fake officials deceive victims, coercing them into divulging sensitive information or visiting specific websites.
- **Culpability and Liability**:
- **Section 66E of IT Act, 2000**: Imprisonment up to 3 years and/or a fine up to ₹2,00,000 and/or **Section 66D of IT Act, 2000**: Imprisonment up to 3 years and a fine up to ₹1,00,000 and/or : Section 66C of IT Act, 2000: Imprisonment up to 3 years and fine up to ₹1,00,000.

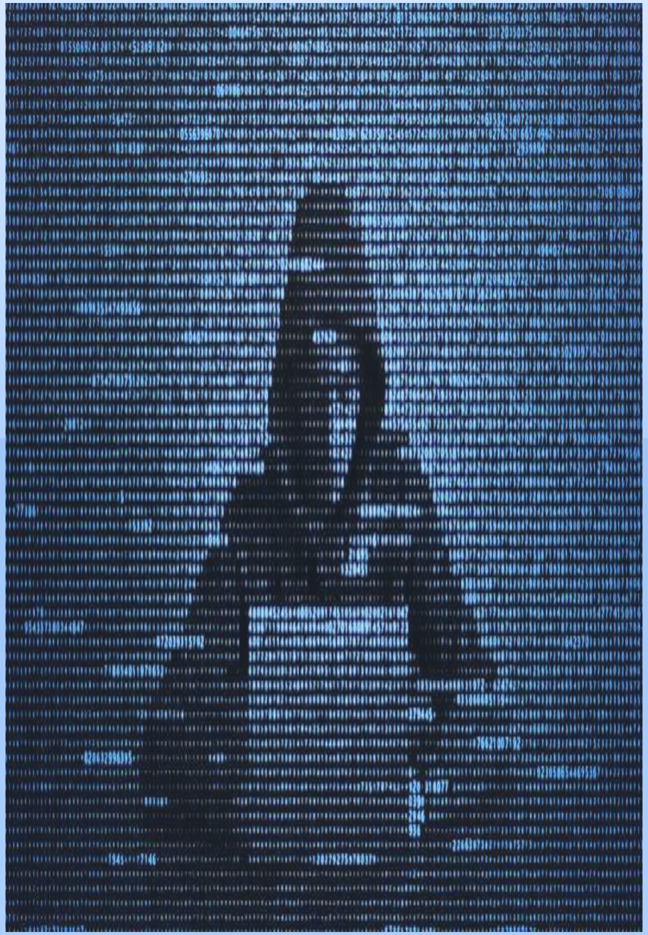


DIGITAL ARREST SCAM



- **Digital arrest menace** is so much on the play that the Hon'ble Supreme Court in its **recent order of 4th Augst 2026** in suo motu proceedings has proposed to the government of India for making it as a stand-alone offense under criminal law, having ingredients of robbery and extortion.
- The good factor however, is that complaints on the national cyber crime reporting portal (as per the report of Indian cyber crime coordination center –I4C)showed that complaints fell from 123,672 in 2024 to 58,249 in 2025 and standing at 16,377 in the first six months of 2026.
- Digital scammers had proved nimble in their modus operandi. They route calls through **SIM** boxes to mask their origin, making them appear as Indian numbers and use multiple mule accounts across many states to move funds swiftly. They are known to deploy deep fakes on video calls to dupe victims and remain untraceable by investigators.
- Even though section 75 of the IT Act 2000 ordains extra territorial jurisdiction, conviction of digital scammers are rare as many of these scams are run from overseas **" Scam compounds"** in Myanmar, the wider golden triangle, and Cambodia. So, the need of the hour is also to use diplomatic pressure to compel these countries to act against the network hosting these scam compounds.

- **Cyberstalking**: Persistent online harassment or monitoring of an individual.
- Culpability and Liability: Section 66E of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹2,00,000.
- **Revenge Porn**: Sharing intimate images or videos without consent to defame or blackmail.
- **Culpability and Liability**:
  - Section 67 of IT Act, 2000: Imprisonment up to 5 years and fine up to ₹10,00,000.
  - Section 67A of IT Act, 2000: Imprisonment up to 7 years and fine up to ₹10,00,000.
- **Cyber Defamation**: Publishing defamatory content about someone online.
- Culpability and Liability: Section 66 of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹5,00,000.
- **Ransomware Attacks**: Encrypting or locking data and demanding ransom for its release.
- **Identity Theft**: Stealing Personal Details to pretend to be someone else.
- **Debit/Credit Card Fraud:** It involves in using an unauthorized use of another's Debit/Credit Card Information for the purpose of purchase or withdrawing funds from it.
- **Espionage:** Act or practice of obtaining data and information without the permission and knowledge of the owner.
- **Pharming**: It's a cyber attack aiming to redirect a website's traffic to another, bogus website .



- **<u>Online Child Sexual Abuse Material (CSAM)</u>**: Creation, transmission, or viewing of sexually explicit content involving children.
- Culpability and Liability: Section 67B of IT Act, 2000: Imprisonment up to 7 years and fine up to ₹10,00,000.
- **<u>Cyber Grooming</u>**: Building a relationship with a child online for the purpose of exploitation or abuse.
- Culpability and Liability: Section 66E of IT Act, 2000: Imprisonment up to 3 years and/or fine up to ₹2,00,000.
- Section 95 of Bharatiya Nyaya Sanhita (BNS), 2023, it penalizes hiring, employing or engaging a child to commit an offence with an imprisonment which shall not be less than 3 years but may extend to 10 years, and with fine.
- **<u>Cyber Bullying</u>**: Harassment, threats, or intimidation of children through online platforms.
- Culpability and Liability: POCSO Act, 2012 prescribes penal provisions based on severity.

- **Dating or Romance Scams**: Deceiving individuals into fake relationships for financial gain or exploitation.
- **Culpability and Liability**: Section 66D of IT Act, 2000: Imprisonment up to 3 years and fine up to ₹1,00,000.
- **Cat Phishing**: Using fake profiles or identities to lure victims into scams.
- **Honey Traps**: Seducing individuals for blackmail or extortion using intimate exchanges.
- Culpability and Liability: Section 67 of IT Act, 2000: Imprisonment up to 5 years and fine up to ₹10,00,000.

DIGITAL PERSONAL DATA PROTECTION ACT,2023

- ❖ DPDP ACT,2023 is India's comprehensive data privacy law. It governs how digital data of individuals is collected, processed and stored. It balances individual privacy rights with the lawful needs of business and government.
- ❖ DPDP ACT,2023 introduces a more general rights-based framework for data protection, requiring explicit consent for the collection, processing, and sharing of personal data. The Act however does not apply to personal data that is "made or caused to be made publicly available". Meaning thereby, the **doxxing** incidents (originated as dropping dox involving publishing private information like phone numbers, addresses, Aadhar details, or photos without consent, often to intimidate or silence) lack direct redressal through specific law and with limited recourse to invocation of provisions under BNS & IT Act,2000.

GOOD SAMARITANS

- ***CERT-In (Indian Computer Emergency Response Team):*** Functions as the national nodal agency for cybersecurity incident response, providing advisories, vulnerability assessments, and coordination for cyber threat mitigation.
- ***Cyber Jaagrookta Campaign:*** Focuses on raising awareness about cyber threats and safety measures through targeted public campaigns.
- ***Cybercrime Reporting Portal (www.cybercrime.gov.in):*** A dedicated platform for citizens to report cybercrimes such as fraud, harassment, and online abuse. It also provides resources to educate users about cyber safety.
- ***National Investigation Agency (NIA):*** Empowers India's fight against terrorism and cyber terrorism through robust investigations, cross-border collaborations, and cutting-edge digital forensics.
- ***'Chakshu' feature on the Sanchar Saathi portal:*** Enabling users to report fraudulent communication, including calls, SMS, and WhatsApp messages designed to deceive users.
- ***Cyber Swachhta Kendra:*** Offers tools for detecting and removing malware, promoting digital hygiene, and protecting devices from cyber threats.
- ***#CyberDost Campaign:*** A public awareness initiative using social media platforms to educate citizens on cyber safety, fraud prevention, and digital literacy.
- Partnerships with International Organizations like INTERPOL, UNODC (United Nations Office on Drugs and Crime), that aligns with the Budapest Convention to strengthen cross-border cybercrime cooperation.
- National Cybersecurity Coordinator (NCTC): Acts as the central body for coordinating all cybersecurity-related efforts and implementing policy frameworks to counter cyber threats.
- National Cyber Forensic Laboratory (NCFL): A facility for forensic analysis and investigation of cybercrime by use of the latest digital technology to support investigations undertaken by Law Enforcement Agencies.

Call
1930

SAFEGUARDS

- **Use Strong Passwords:** Combine uppercase, lowercase, numbers, and symbols.
- **Enable Two-Factor Authentication (2FA):** Add an extra layer of security.
- **Keep Software Updated:** Install updates and patches regularly.
- **Avoid Clicking Unknown Links:** Be cautious of phishing emails and suspicious links.
- **Use Antivirus and Firewalls:** Protect devices with reliable security tools.
- **Secure Wi-Fi Networks:** Use strong passwords and avoid public Wi-Fi.
- **Backup Data Regularly:** Store backups offline or on secure cloud platforms.
- **Be Mindful of Sharing Information:** Limit sharing sensitive data online.
- **Monitor Financial Transactions:** Check bank statements for unauthorized activity.
- **Educate Yourself:** Stay informed about common cyber threats.
- **Monitor your bank Statements .**
- **Protect your Personal information online .**

FOCUS

- **Prevention** is better than Cure.
- **Digital Austerity** is the mantra for attaining peace and avoiding digital entanglement(s).
- **Responsible internet use** is panacea for digital age-related malaise.
- **Awareness** is the best defense against cyber crime.


THANK YOU