Cyber Crimes:
Emerging Jurisprudence and Judicial Response

By: M K Sil

25-April-2025

Cybercrime – as we define

Cybercrime refers to any unlawful act where computers, networks, or digital systems are used as tools, targets, or means to commit offenses, such as fraud, data theft, unauthorized access, or disruption, in violation of applicable laws.

Cybercrime encompasses unauthorized system access, identify theft, online scam – A wide range of offences

- **Unauthorized access** to or **Hacking** of computer systems and networks.
- **Data theft**, identity theft, and information breaches.
- **Cyber fraud**, including **Phishing**, online scams, and financial crimes.
- **Distribution of malware**, ransomware, spyware, and viruses.
- **Cyberstalking**, online harassment, and defamation.
- **Denial-of-Service (DoS) and Distributed DoS (DDoS)** attacks disrupting services.
- **Intellectual property theft** and software piracy.
- **Online child exploitation** and dissemination of illegal content.
- **Cyberterrorism**, including attacks on critical infrastructure.

Cybercrime is a rapidly growing area of crime, with an increasing number of criminals exploiting the speed, convenience, and anonymity of the internet to commit a wide range of offenses that transcend both physical and virtual borders.

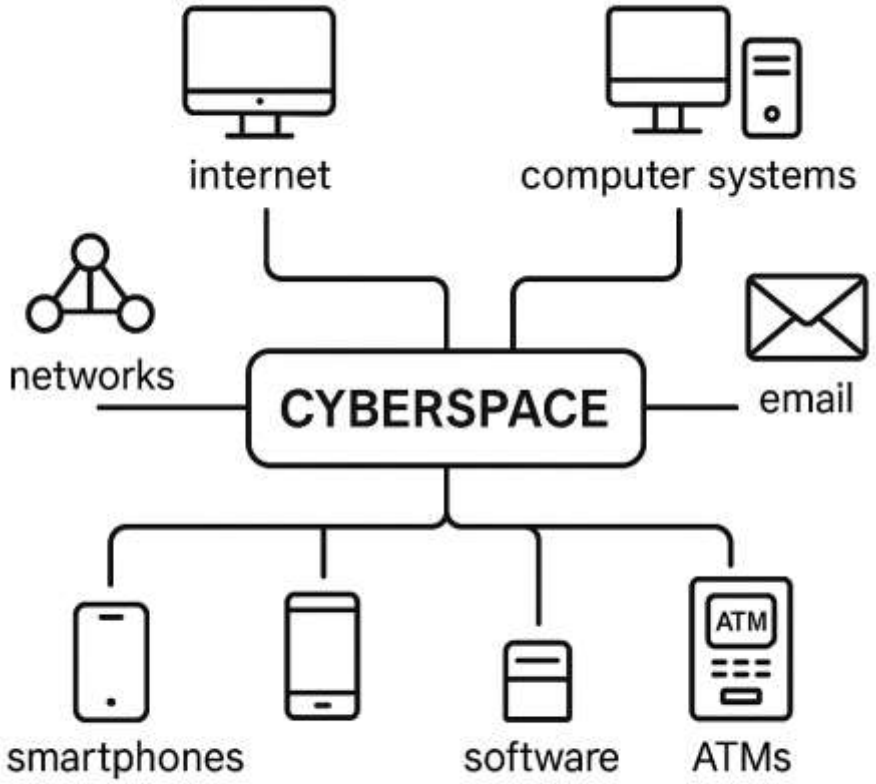
- **Phishing** attacks work by deceiving you into entering your username and password on a fake website that mimics your bank, broker, or employer.

- **Malware** is malicious software designed to disrupt, damage, or gain unauthorized access to systems. It includes viruses, worms, Trojans, ransomware, and spyware, spreading through phishing, downloads, or system vulnerabilities.

- **Spyware** is malicious software that secretly monitors and collects user data, such as passwords, browsing habits, and personal information, without consent. It often spreads through phishing, software downloads, or security vulnerabilities.

Cyberspace refers to the interconnected network of information technology infrastructure, including the internet, computer systems, embedded processors, and controllers.

Broadly, it encompasses computers, networks, software, emails, and electronic devices such as smartphones and ATMs.



Cyberspace is the digital ecosystem enabled by the internet and interconnected networks, encompassing communication, commerce, finance, data storage, and governance. It is both a platform for innovation and a domain vulnerable to cybercrime.

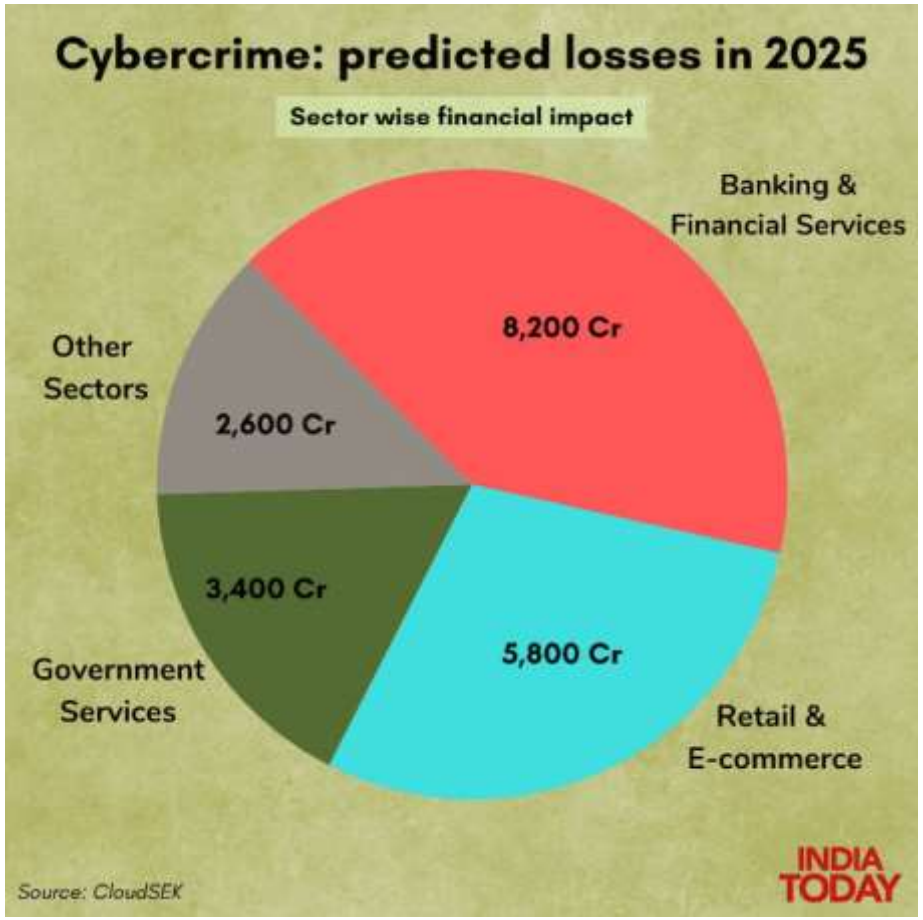
- **Social Media** (e.g., Facebook, Twitter, Instagram): Key platforms for communication and public discourse; often relevant in cybercrime investigations.
- **Messaging Apps** (e.g., WhatsApp, Telegram, Signal): Enable encrypted, real-time communication; frequently used in both lawful and illicit activities.
- **E-Commerce** (e.g., Amazon, eBay, Alibaba): Facilitate online trade; also exploited for fraud, counterfeit goods, and scams.
- **Cloud Storage** (e.g., Google Drive, OneDrive, Dropbox): Allow remote data access; important for digital evidence and also vulnerable to data breaches.
- **Online Banking**: Supports digital financial transactions; targeted by fraud, phishing, and money laundering schemes.
- **Online Entertainment & Gaming**: Platforms that can be misused for illegal streaming, financial fraud, or exploitation.
- **E-Governance Portals**: Used for services like tax filing and customs; potential targets for cyberattacks and data theft.

Evolving Legal landscape on cyber crime

- **Cybercrime is rapidly evolving**, necessitating a robust and responsive legal and enforcement framework to effectively combat emerging threats.

- **The Legal landscape in India** needs to continuously adapt to emerging Cyber threats by strengthening legislation updating the existing laws & introducing new regulations to address the complexities of modern-day cyber crime.

- **Statutory Framework for Cybercrime in India**:
  The Bharatiya Nyaya Sanhita (BNS) (formerly Indian Penal Code) and the Information Technology Act, 2000 (amended in 2008 and 2023) together form the core legal framework for addressing cybercrime, providing substantial provisions for investigation, prosecution, and regulation of cyber offenses.

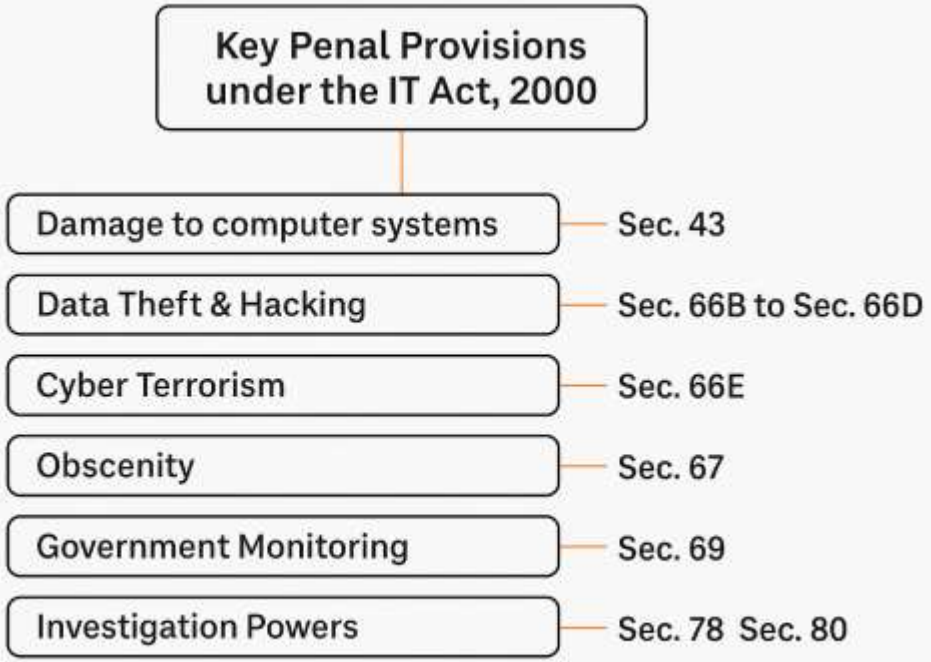


The IT Act, 2000 & the BNS together form the comprehensive legal framework for addressing cybercrime in India. These statutes provide both procedural and substantive provisions to combat various forms of cyber offenses.

A few important provisions under I T Act 2000 & IPC in combating cybercrime as given below

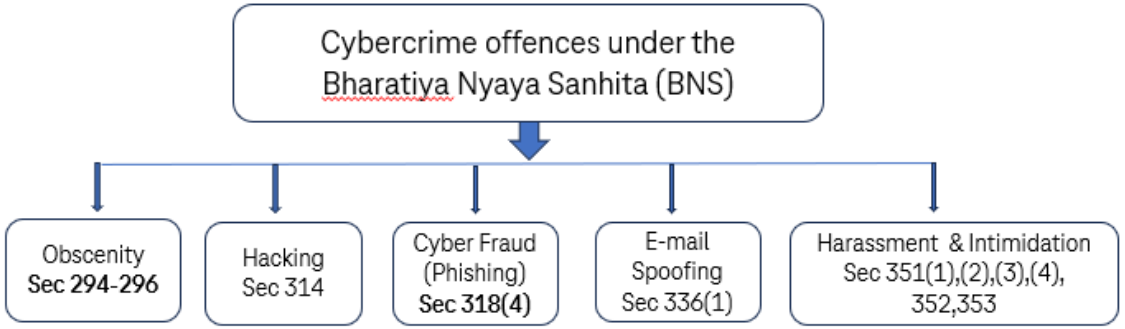
Key Penal Provisions under the IT Act, 2000

- **Section 43** – Unauthorized access and damage to computer systems or data
- **Sections 66B to 66D** – Data theft, identity theft, and hacking related offenses
- **Section 66E** – Cyber terrorism and violation of privacy
- **Section 67** – Publishing or transmitting obscene material, including child pornography
- **Section 69** – Government's power to intercept, monitor, or decrypt digital information for national security
- **Section 78** – Powers conferred to officers for investigating cyber offenses
- **Section 80** – Power of police officers to enter, search, and arrest without warrant in certain cybercrime cases



Relevant Provisions under the BNS (Formerly IPC)

- **Sections 294,295,296** – Obscenity and publication of obscene content
- **Section 314** – Dishonest misappropriation of property (applicable to hacking-related offenses)
- **Section 318(4)** – Cheating and dishonestly inducing delivery of property (applicable to phishing and fraud)
- **Section 336(1)** – Forgery, relevant to email spoofing and falsification of digital records
- **Sections 351(1),(2),(3),(4), 352,353** – Criminal intimidation, threats, and harassment through digital means



Supplementary Legal and Policy Measures for Combating Cybercrime in India

There are various other laws / rules /guidelines wherein monitoring, detection, prevention, mitigation & management measures have been established to combat cyber crime in India

Policy & Regulatory Measures:

- **National Cyber Security Policy, 2023** – Strategic framework for securing national digital infrastructure.
- **IT (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2025** – Regulates online content and intermediary responsibilities.
- **National Cyber Crime Reporting Portal** – Enables public reporting of cybercrime incidents, launched by central government
- **CERT-In** – Coordinates incident response and international cyber investigations.

Sector-Specific guidelines:

- **IT Services Outsourcing Directives, 2023 (PPP Model)** – Ensures secure handling of outsourced IT services.
- **TRAI Recommendations (2018)** – Addresses privacy, data security, and ownership in telecom.
- **RBI Master Directions** – Mandates IT governance and risk control for financial institutions and Assurance practices.
- **Companies (Management and Administration) Rules, 2014** – Prescribes digital compliance and data security for corporations.

Additionally, the **IT Act, 2000 (as amended in 2025)** is now supplemented by procedural laws under the **Bhartiya Nagarik Suraksha Sanhita** (formerly CRPC) , which governs the **investigation and prosecution** of cybercrime cases.

International Treaties on Cybercrime – India's Engagement

The **United Nations General Assembly**, with consensus from all **193 member states**, has adopted a **landmark convention on cybercrime**—the first legally binding international treaty addressing cybercrime. This convention aims to enhance **global cooperation** in preventing, investigating, and prosecuting cyber offenses such as **online child exploitation**, **money laundering**, and **financial fraud**.

Key Objectives of the UN Convention on Cybercrime:

- **Strengthen international cooperation** in combating cybercrime through joint legal and technical mechanisms.
- **Facilitate investigation and prosecution** of cyber offenses, including the ability to **freeze, confiscate, and return proceeds of crime**.
- **Support cross-border evidence collection and sharing** of electronic evidence in criminal investigations.
- **Promote mutual legal assistance**, extradition arrangements, and real-time communication through a **24x7 international cybercrime cooperation network**.

India’s Bilateral and Multilateral Engagements:

- In **2015**, India signed an **MoU with Germany** on **Security Cooperation**, which includes provisions related to combating cybercrime.

- In **2016**, India entered into **cybersecurity MoUs with Singapore, Malaysia, and Japan**, focusing on cyber threat intelligence sharing, capacity building, and coordinated response mechanisms.

Conclusion

- In the face of rapidly evolving cyber threats, India has developed a multi-layered legal, regulatory, and institutional framework to combat cybercrime. The convergence of the **IT Act, 2000 (as amended)**, the **Bharatiya Nyaya Sanhita**, and various **sectoral policies and international agreements** reflects a robust national commitment.

- A well-informed, tech-savvy, and responsive judicial system is essential to ensure effective enforcement, protect digital rights, and uphold the rule of law in cyberspace.

Thank You