Cybercrime Legislation in India: Detailed Analysis of Statutory Provisions

Authors: Krishna CV Grandhi, Chandra Lekha

The legal framework governing cybercrimes in India is spread over a web of interconnected legislations. The primary statute on the question of cybercrimes is the Information Technology Act, 2000 ("IT Act") which works in conjunction with criminal legislations like the Bharatiya Nyaya Sanhita, 2023 (BNS)(erstwhile Indian Penal Code), Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)(erstwhile Code of Criminal Procedure), Bharatiya Sakshya Adhinayam, 2023 (BSA)(erstwhile Indian Evidence Act), along with provisions of the Digital Personal Data Protection Act, 2023 which is yet to come into force.

Information Technology Act, 2000: Core Cybercrime Provisions

Primary Offences (Sections 65-67B)

Section 66 is the primary provision for cybercrime prosecution, criminalizing computer-related offenses carried out through fraud. Such offences hacking, data theft, and DDoS attacks, with punishment extending to three years imprisonment or ₹5 lakh fine.

Identity and Impersonation Crimes:

- **Section 66C (Identity Theft):** Section 66C deals with any malicious use of electronic signatures, passwords or other biometric identifiers. An offence under this section is punishable with imprisonment of three years and a fine of ₹1 lakh.
- **Section 66D (Cheating by Personation):** This Section deals with the use of computer resources to impersonate other persons in order to carry out fraudulent activities and is punishable with imprisonment of three years and a fine of ₹1 lakh.

Privacy and Harassment Offenses:

- **Section 66E (Privacy Violation):** Section 66E deals with the unauthorised capturing or publishing images of a person's private areas. Offences under this section are punishable with imprisonment of three years along with a fine of ₹2 lakh.
- **Section 66F (Cyber Terrorism):** Offences under Section 66F are considered a grievous offences targeting the national security of the country. Any individual convicted under this section is punishable with imprisonment for life.

Obscenity and Offences related to Children (Sections 67-67B)

- **Section 67:** General obscene material publication. Such offences are punishable with imprisonment of 3-5 years and a fine of ₹5-10 lakh.
- **Section 67A:** Publication of sexually explicit content may be punishable under the IT Act with imprisonment of 5-7 years along with a fine of ₹10 lakh.
- **Section 67B:** Under the IT Act, publication of child exploitation material including creation, distribution of such material, and inducement of a child for online relationships are punishable with imprisonment up to 5-7 years and a fine of ₹10 lakh.

Government Powers and Infrastructure Protection (Sections 69-70B)

Sections 69-69B: This provision grants government agencies extensive surveillance and blocking powers for the purposes of national security, public order, and cybersecurity. Any non-compliance by any intermediary or person-in charge of a computer resource under this section may attract a penalty up to one year of imprisonment along with a fine of ₹1 Crore.

Section 70: Section 70 empowers the government to designate any computer resource that may impact the 'Critical Information Infrastructure of the country as 'protected systems.' Any unauthorised use of such designated systems may be punishable with imprisonment up to 10 years.

Procedural and Enforcement Provisions

Section 78: Section 78 of the IT Act mandates that a cybercrime investigation may not be conducted by any police officer below the rank of an Inspector,

Section 80: Section 80 of the IT Act also provides the police the power to arrest and search in public places without a warrant.

Traditional Criminal Law Integration

Indian Penal Code/Bharatiya Nyaya Sanhita Provisions

Gender-Based Cybercrimes:

- **Section 354A/75 (Sexual Harassment):** The section penalises online sexual harassment including unwelcome advances, pornography display, and making any sexually coloured remarks. An offence under this section is punishable with imprisonment between 1-3 years.

- **Section 354C/77 (Voyeurism):** This provision penalises the unauthorized recording and dissemination of private acts wherein a person would usually have the expectation of not being observed by any other person. Such an offence is punishable with imprisonment between 1-7 years based on conviction history of the accused.
- **Section 354D/78 (Stalking):** Includes monitoring electronic communication and repeated unwanted contact (3-5 years)

Communication Offenses:

- **Section 499/356 (Defamation):** Covers online reputation damage through false imputations (up to 2 years)
- **Section 507 (Anonymous Criminal Intimidation):** Enhanced punishment for threats through untraceable means
- **Section 353 (BNS - Public Mischief):** Criminalizes false information likely to cause public alarm or communal discord, particularly relevant for social media misuse

Substantive Overlap and Charging Strategy

Cybercrimes often invoke multiple statutes simultaneously. For example, an online impersonation fraud may attract Section 66D of the IT Act in addition to Sections 419 (cheating by impersonation) and 420 (cheating) of the IPC thereby ensuring a comprehensive coverage and redressal.

Procedural Framework

Investigation and Evidence

Criminal Procedure Code/BNSS Sections 156, 175 empower police investigation without magistrate orders for cognizable cybercrimes. **Sections 100-102/103-106** govern search, seizure, and property handling with specific safeguards for electronic evidence.

Admissibility of Electronic Evidence: The Indian Evidence Act/Bharatiya Sakshya Adhiniyam **Sections 65B/63** establish the foundation for digital evidence admissibility, requiring certification that:

- Computer systems operated properly during relevant periods
- Information was regularly fed in ordinary course of activities
- Output accurately reproduces stored information
- Person in charge provides authentication certificate

Specialized Protection Frameworks

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

Section 14 of the POCSO Act addresses child exploitation through pornography, with enhanced punishments of imprisonment between 5-7 years and ensures cumulative charging when combined with direct sexual assault. Section 15 of the POCSO Act criminalizes possession and storage of child exploitation material with commercial purpose attracting 3-7 years imprisonment.

Digital Personal Data Protection Act, 2023

While DPDPA is yet to come into force, it is a significant legislation with respect to the question of online privacy and creates indirect protection against AI-driven cyber threats through:

- Consent and purpose limitation preventing unauthorized data use for harmful AI applications
- Breach notification requirements ensuring accountability for data misuse
- Additional obligations are imposed on entities designated as Significant Data Fiduciaries including mandatory appointment of Data Protection Officers and conducting regular audits of the personal data collected.

Jurisdictional and Enforcement Mechanisms

Section 75 of the IT Act also extends jurisdiction to offences committed outside the jurisdiction of India if they include computer system based in India. Section 85 of the IT Act further establishes corporate liability thereby making companies and individual officers of the company accountable for any cybercrimes committed under the company's name.

Law enforcement agencies operate at multiple levels during the course of a cyber crime investigation:

- Local police investigate routine cybercrimes alongside the state cyber cells.
- Central agencies like the Central Bureau of Investigation and National Investigation Agency undertake investigation for serious offenses affecting national security.
- Specialized units like Indian Computer Emergency Response Team (CERT-In) conduct investigations along with other law enforcement agencies upon receiving information of an offence or incident.

Legal Integration and Challenges

The multi-statutory and multi-agency approach ensures comprehensive and cumulative charging of cyber offences. However, such decentralisation also leads to complexities in prosecution and at times, simultaneous investigations leading to lack of proper and timely trial of the perpetrators.

These gaps become further evident in investigations of AI-driven crimes wherein traditional legislations and investigative methods are outpaced by perpetrators who exploit technologies such as automated decision-making, algorithmic bias, and sophisticated social engineering attacks that blur traditional offence categories. Evolution of the current legal landscape and investigative techniques is necessary to address the emerging technological challenges while maintaining the existing integrated framework.

www.csail.org