JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Rise of Cybercrime in India: Understanding the Emerging Threats

Author- Divyanshi Raj
Legal Associate
Integra Law Office, New Delhi

Abstract

Cybercrime in India has evolved into a serious national concern, worsen by rapid digitization, growing internet penetration, and digital financial inclusion. This article examines the surge in cybercrimes, analyses the current legal frameworks governing cyber activities, explores key judicial interpretations, and investigates emerging cyber threats such as ransomware, Al-driven fraud, and crypto-based laundering. It concludes with targeted recommendations for legislative and policy reform.

Introduction

India's digital transformation, accelerated by initiatives like Digital India, has led to an unprecedented rise in the use of electronic platforms for communication, banking, commerce, and governance. With this growth has come a parallel and concerning rise in cybercrime. From online scams and phishing attacks to state-sponsored hacking, the country's cyber landscape is under siege.

Over 740,000 cases of cyber crime were reported to the Indian Cyber Crime Coordination Centre (I4C) in India within first four month of 2024 alone[1]. The number of cyber crimes in the country saw a massive spike between 2019 and 2020 and have been on the rise ever since. Roughly 85 percent of the reports in 2024 were related to online financial frauds. The National Crime Records Bureau (NCRB)[2] reported over 65,000 registered cybercrime cases in 2022 alone—a figure that likely underrepresents the true scale due to underreporting and lack of awareness.

[1] *Cyber Crime in India-statistics & facts (2024),* https://www.statista.com.
[2] National Crime Record Bureau, *Crime in India-2022 Statistics*, Ministry of Home Affairs, Govt. of India (2023), https://ncrb.gov.in

Understanding Cybercrime in the Indian Context

Cybercrime can be defined as any unlawful act committed using a computer or digital device as either a tool, a target, or both. The most prevalent forms of cybercrime in India[3] include:

- Financial Fraud

  Cybercriminals exploit online banking systems, UPI platforms, and digital wallets through phishing, fake websites, and SIM swapping.
- Identity Theft

Data leaks and poor cybersecurity allow attackers to impersonate users, access financial systems, and commit fraud.

- Cyberstalking and Harassment

The anonymity of the internet facilitates online abuse, revenge porn, and threats, often targeting women and children.

- Cyberterrorism and Espionage

Attacks on critical infrastructure such as healthcare, power grids, and military installations have been linked to foreign actors.

Legal Framework in India

India has enacted several legal provisions to combat cybercrime, the most prominent being the Information Technology Act, 2000[4], which has been amended over time to include various offenses.

❖ **The IT Act, 2000**

- Section 66C: Identity theft
- Section 66D: Cheating using communication devices
- Section 67: Publishing or transmitting obscene material
- Section 70B: Empowering CERT-IN to monitor cyber incidents

❖ **Indian Penal Code (IPC)[5] now Bharatiya Nyaya Sanhita (BNS)[6]**

- Cheating and dishonestly inducing delivery of property Section 420 of IPC now Section 318 of BNS.
- Criminal defamation Section 500 of IPC now Section 356 of BNS.

[3] Samyukta V & Devarajan, *Emerging Cyber Threats in India: A Wake-Up Call for Legal Reforms, Indian J. Law & Legal Reforms* (2023), https://ijllr.com
[4] The Information Technology Act, 2000 (No. 21 of 2000), ss. 66C,66D,67,70B.
[5] The Indian Penal Code, 1860 (No. 45 of 1860), ss.354D,420,500.
[6] The Bharatiya Nyaya Sanhita, 2023,(No. 45 of 2023), ss.78,318,356.

- Cyberstalking Section 354D of IPC now Section 78 of BNS.

❖ **The Digital Personal Data Protection Act, 2023**

While not yet fully implemented, this act seeks to strengthen protection of personal data and privacy rights, an essential aspect in combating cybercrime[7].

Emerging Threats in India's Cyber Space

- Ransomware-as-a-Service (RaaS)
  Attacks like the AIIMS-Delhi ransomware incident (2022) demonstrate the vulnerability of even well-protected systems.
- Deepfake Technology
  Al-generated fake videos and audios are being used for character assassination, blackmail, and misinformation.
- Cryptocurrency and Money Laundering
  Digital currencies are increasingly used to fund illicit transactions due to their anonymity.
- Dark Web Markets
  Cybercriminals trade stolen data, hacking tools, and malware on encrypted networks that evade traditional surveillance.

Challenges in Combating Cybercrime

- Jurisdictional Conflicts: Cybercrimes often transcend national borders, making investigation and enforcement difficult.
- Lack of Digital Literacy: Many users are unaware of basic cybersecurity practices
- Inadequate Police Training: Law enforcement often lacks specialized skills or technology to track and investigate cybercrimes.
- Delayed Legislative Updates: Laws have not kept pace with fast-evolving digital threats.

Judicial Trends and Key Cases

Indian courts have begun to interpret cyber laws in light of evolving technology:

- Shreya Singhal v. Union of India (2015)[8]
  This landmark case challenged the constitutionality of Section 66A of the Information Technology Act, 2000, which penalized sending "offensive messages" through communication services. The Hon'ble Supreme Court

[7] The Digital Data Protection Act, No.22 of 2023, Ministry of Electronics and Information Technology, https://www.meity.gov.in
[8] Shreya Singhal v. Union of India (2015) 5 SCC 1 (India)

struck down the Section 66A of the IT Act as unconstitutional for violating freedom of speech and expression under Article 19(1)(a) of the Constitution.

- Dr. R.K Chauhan v. State of U.P. (2010)[9]

  This case highlighted the importance of digital privacy. The Hon'ble Court held that unauthorized access to person's email account constitutes an offence under Section 66 of the Information Technology Act, 2000.

- Manik Taneja v. State of Karnataka (2015)[10]

  The Hon'ble Supreme Court held that posting public criticism does not constitute oran offence under defamation laws.

- Aaradhya Bachchan v. YouTubers (2023)[11]

The Hon'ble Delhi High Court ordered YouTube and Google to take down defamatory content and emphasized platforms duty to moderate harmful content and it highlighted the need for protection against online defamation and cyberbullying of minors.

Recommendations

- Legal Reform: Update the IT Act and IPC to include new threats like Al, lot misuse, and crypto-related offenses.
- Capacity Building: Establish specialized r cells in every district with trained personnel and forensic tools.
- Public Awareness: Launch nationwide digital hygiene and cybercrime reporting campaigns.
- International Cooperation: Strengthen treaties and data-sharing frameworks for cross-border cybercrime investigation.

Conclusion

As India advances digitally, the threat of cybercrime grows more pronounced and complex. Though legislative frameworks like the IT Act provide a starting point, they are no longer sufficient in isolation. Tackling cybercrime in India requires a synchronized response involving law reform, institutional strengthening, and public engagement. The need of the hour is a robust, adaptive, and human-rights-sensitive legal architecture that can respond dynamically to emerging threats.

Cybercrime in India is not only a digital challenge but also a constitutional and human rights issue. The current legal architecture must be upgraded to match the sophistication of emerging threats. Judicial vigilance, legislative foresight, and institutional reform are key pillars for a secure digital India.

[9] Dr. R.K Chauhan v. State of U.P. (2010) Cri LJ 1267
[10] Manik Taneja v. State of Karnataka (2015) 7 SCC 423
[11] Aaradhya Bachchan v. YouTubers (2023) SCC OnLine Del 3569