

Jurisprudential challenges in cybercrime adjudication

- Legal complexities in prosecuting cyber offenses
- Evolving judicial interpretations and precedents

By: M K SIL
25-Apr-2025

Jurisprudential Hurdles - Explanation

- The rapid expansion of India's digital ecosystem has led to a parallel rise in cybercrimes across sectors – banking, governance, healthcare, and personal data privacy.
- The IT Act, 2000, remains the cornerstone, serves as India's primary legislative framework to combat cyber offenses.
- Members of the judiciary are increasingly required to interpret complex cybercrime cases involving technical evidence, cross-border jurisdictional issues, and interpretative challenges under evolving legal frameworks.
- Limited Judicial Precedent: Cyber jurisprudence is still evolving, with relatively few guiding case laws on emerging technologies.

Legal Intricacies in Enforcement

- **Digital Evidence Admissibility:** Section 65B of the Indian Evidence Act requires strict certification for electronic records, often a hurdle in court.
- **Jurisdictional Overlaps:** Offenses often invoke both the IT Act and IPC, leading to confusion over applicable provisions and forum.
- **Cross-Border Challenges:** Many cybercrimes originate outside India, complicating investigation and prosecution.
- **Lack of Uniform Interpretation:** Inconsistent application of cyber laws across jurisdictions due to limited cyber-specialized courts.

Key Issues in Cybercrime Adjudication

- **Technological Evolution:** Law often lags behind fast-paced tech advancements.
- **Ambiguous Definitions:** Difficulty in interpreting legal provisions due to undefined or broad terminology.
- **Jurisdictional Dilemmas:** Crimes often originate from one country and affect individuals or systems in another.
- **Admissibility of Digital Evidence:** High technical standards for compliance under Indian Evidence Act.

Jurisprudential Challenges

Vague Legal Language: Section 66 of the IT Act uses broad terms like "dishonestly" or "fraudulently," open to subjective interpretation.

Interpretative Ambiguity: For instance, in unauthorized access or hacking cases, it remains unclear whether mere access without demonstrable malicious intent constitutes a punishable offense.

Mens Rea in Cyber Offenses: Determining intent is particularly challenging in cyber offenses where acts may be automated, executed remotely, or obscured by digital anonymity.

(Mens Rea : meaning a culpable mental state or criminal intent)

Traditional Doctrines Misfit: Conventional legal concepts such as physical possession, direct causation, or tangible harm often do not align with the virtual nature of cybercrimes, complicating adjudication.

Key legislation - Role of judiciary - Interpretation

Investigating power to address Cyber Security, Terrorism and other Criminal activities in India.

The key legislations are

- • The Information Technology Act
- • The unlawful Activities Prevention Act (UAPA) 1967
- • The Bharatiya Naya Sanhita (BNS) formerly IPC
- • The Bharatiya Nagarik Surakhsa Sanhita
- • Digital Personal data Protection Act 2023

Powers for investigation / enquiry (formerly CrPC)

Key Legal Provisions for Cybercrime Investigation

- **Section 69 - IT Act, 2000:** The Govt issues directions for interception, monitoring or decryptions of any information through any computer resource if it is reasonable to do so in the public interest.
Grounds: Sovereignty and Integrity of the State; public order or preventing incitement to the commission of any cognizable offence.
- **Section 43A - UAPA, 1967:** DSP-level officers empowered to **arrest, investigate, and detain** suspects in terrorism-related cyber activities.
- **Section 91 - CrPC / BNSS:** Empowers a Court or an officer in charge of a P.S. to issue summon to provide any document or electronic record for the purpose of investigation..
- **Section 78 - IT Act, 2000:** **Police Inspector or above** authorized to investigate offenses under the IT Act.
- **Section 80 - IT Act, 2000:** **Police Inspector or above** can **enter, search, and arrest** without warrant in public places for IT Act offenses.

DPDPA - Powers of the Data Protection Board (Section 18)

Sec 18 envisage that Govt. will constitute the **Data Protection Board of India (DPBI)** and would function and shall have the same power as one vested in a Civil Court under the Code of Civil Procedure 1908 (as amended by Code of Civil procedure Amendment Act 2022) in the matter relating to

- Summoning and enforcing the attendance of any person and to examine them under oath
- To produce documents relevant to inquiries
- To inspect any data, book, documents, registers, accounts etc which the office asked for / prescribed.
- DPBI is also empowered to adjudicate the offences relating to IT Act violations, and cybercrimes.

Role of the Judiciary in Cybercrime Adjudication

The judiciary plays a crucial role in cybercrime by interpreting and applying cyber laws,

- Ensuring fair trial, upholding constitutional safeguard including right to freedom of speech and expression and recognizing digital space (cyber space),
- Adapts legal reasoning to the evolving nature of cybercrime.
- Addresses cases involving digital arrest scams, online job frauds, and investment scams, often resulting in significant financial loss to victims.
- Judgement often involve imprisonment and fines for the offenders with the I.T Act being the primary legal framework for such adjudication.

Few recent cyber crime cases in India and their judgements

Reference: *Cyber Crime and the Court: Judicial Insights in India and Beyond. International Journal of Research and Analytical Reviews (IJRAR), Vol. 11, Issue 4, October 2024. Dr. Vijaykumar Sriasshen Chowbe.*

Notable cases cited

- **State of Punjab vs M/s Amritsar Beverage Limited:**
(Jurisdictional and evidentiary implications in digital transaction disputes)
- **Shreya Singhal vs Union of India:**
(Landmark judgment striking down Section 66A of the IT Act on grounds of free speech)
- **Manik Taneja vs State of Karnataka:**
(Examined the scope of online criticism and its intersection with defamation and misuse of power)
- **Sanjay Kumar vs State of Haryana:**
(Involved digital evidence and procedural fairness in a cyber fraud case)

Notable Cyber Law Case Studies

Source: CLS Cyber laws and Information Security Advisors Important cyber law case studies.
Notable cases cited


- **Sony Sambandh.com Case:** Involved data theft and breach of customer information by an insider.
- **Bank NSP Case:** Concerned breach of confidentiality and misuse of sensitive information in an online banking context.
- **Bazee.com Case:** The CEO of Bazee.com was held liable for obscene content sold via the platform –highlighted intermediary liability.
- **BSNL Unauthorized Access Case:** A case of illegal access and tampering with BSNL's internal systems, demonstrating weaknesses in public sector digital infrastructure.
- **Digital Arrest Scams: Mumbai Incident** - An 86-year-old woman was extorted of ₹20 crore through a fake “digital arrest” scam, reflecting the emotional and financial impact of cybercrime on vulnerable individuals.

(Ref: Cyber Crime Cases in India and Their Judgments)


Cybercrime Investigation & Importance of Effective Electronic Management

Source: Ref Cybersecurity & Privacy Journal.

Notable cases cited



The Shifu App Case : In the Shifu App case, a notorious banking Trojan named Shifu infected numerous computers, leading to financial fraud. Law enforcement agencies collaborated with cybersecurity experts to investigate the case. Through meticulous electronic evidence collection and preservation, including network traffic analysis and forensic examination of infected systems, investigators successfully traced the origins of the malware and identified the perpetrators. The use of advanced digital forensics techniques and collaboration between law enforcement and technical experts played a crucial role in this investigation.




The Delhi University Exam Scam Case : The Delhi University Exam Scam case involved a cybercrime syndicate that hacked into the examination systems to manipulate exam results. Investigators faced the challenge of collecting electronic evidence from various servers and devices. They employed forensic imaging and seized key digital evidence, such as log files, databases, and communication records. The proper handling and preservation of electronic evidence enabled investigators to reconstruct the chain of events and establish the involvement of the accused individuals.


Cybercrime Investigation & Importance of Effective Electronic Management

Source: Ref Cybersecurity & Privacy Journal.


Notable cases cited



The IPL Spot-Fixing Case : The IPL Spot-Fixing case involved a high-profile cricket betting scandal. Law enforcement agencies, with the assistance of digital forensic experts, collected electronic evidence from mobile phones, laptops, and communication networks. The investigators extracted call records, text messages, and financial transactions, which served as crucial evidence in establishing the involvement of players, bookies, and other individuals. The effective management of electronic evidence played a pivotal role in exposing the illegal activities and ensuring successful prosecutions.



The Wannacry Ransomware Case : The Wannacry ransomware attack affected organizations worldwide, including some in India. Investigating this case required coordination between Indian law enforcement agencies and international authorities. Electronic evidence, such as encrypted files and ransom payment transactions, had to be carefully collected and preserved. Digital forensics experts played a significant role in decrypting files, analysing malware samples, and tracing financial transactions, which helped identify the perpetrators involved in the attack. International cooperation and expertise in electronic evidence management were critical in resolving this case.



These case studies highlighted the importance of effective electronic evidence management in cybercrime investigations. Timely identification and preservation of digital evidence, adherence to legal requirements, collaboration among stakeholders, and the utilization of digital forensics techniques and tools are key factors for the successful investigations.

Challenges in Cybercrime Investigations (India)

Outdated Legal Framework: Existing laws often lag behind evolving cyber threats, necessitating periodic review and reform.

Lack of Specialized Units: Many enforcement agencies lack dedicated cybercrime cells with trained personnel and digital forensic capabilities.

Jurisdictional Complexities: Cybercrimes often span multiple states or countries, complicating investigation and prosecution.

Limited International Cooperation: Challenges persist in extraditing cybercriminals and sharing cross-border digital evidence due to legal and diplomatic hurdles.

Challenges in Handling Extra-Territorial Evidence



Jurisdictional Barriers: Data often resides on servers located in foreign countries, outside Indian legal reach.



Delayed Access: Mutual Legal Assistance Treaties (MLATs) are slow and bureaucratic, delaying investigations.



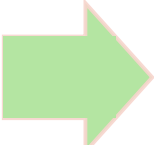
Lack of Harmonized Laws: Variations in privacy, data protection, and evidentiary standards hinder cooperation.




Non-Cooperative Entities: Some foreign service providers may refuse data disclosure due to local laws or lack of bilateral agreements.

Safeguarding Judicial Institutions from Cyber Threats

Cybersecurity Risks to Court Systems

- 
- **Unauthorized access** to digital case files and confidential judicial records
 - **Malware/ransomware attacks** targeting e-court platforms and servers
 - **Data breaches** involving sensitive litigant information
 - **Disruption of digital court proceedings** via DDoS or phishing attacks

Best Practices & Legal Framework

- 
- **Adoption of strong cybersecurity protocols:** firewalls, encryption, multi-factor authentication
 - **Regular audits and vulnerability assessments** of court IT infrastructure
 - **Capacity building and training** for judicial staff on cyber hygiene
 - **Legal safeguards:**
 - **IT Act, 2000** - provides legal recognition and protection for digital records
 - **DPDPA, 2023** - ensures secure handling of personal data
 - **CERT-In guidelines** - mandate incident reporting and cybersecurity compliance



CASE STUDIES

Sec 66A: Punishment for Sending Offensive Messages through Communication Service

- Mouthshut.com vs Union of India was a writ petition filed by the consumer review platform Mouthshut.com and its founder Faisal Farooqui, seeking to protect the right to freedom of speech and expression on the internet. The petition challenged the constitutionality of Section 66A of the Information Technology Act and sought its modification or repeal

Section 43 - Penalty and Compensation for Damage to Computer Systems

- In a landmark 2013 adjudication under Section 43 of the Information Technology Act, one of the largest compensations for a cybercrime dispute was awarded. Maharashtra's IT Secretary, Rajesh Aggarwal, ordered Punjab National Bank (PNB) to pay ₹45 lakhs as compensation to the complainant, Manmohan Singh Matharu, Managing Director of Pune-based firm *Poonam and Ancillaries*.
- The case involved a phishing attack in which a fraudster illicitly transferred ₹80.17 lakhs from Matharu's account in PNB after he unknowingly responded to a phishing email. While the complainant was initially asked to share liability for having responded to the fraudulent email, the bank was ultimately held negligent. The adjudicating authority found that PNB had failed to conduct proper due diligence and security checks when opening and operating the fraudulent account, thereby failing to protect the complainant.



Section 65 - Tampering with Computer Source Documents

Punishable by up to 3 years imprisonment or ₹2 lakh fine, or both, for knowingly altering, concealing, or destroying computer source code required by law.

- Syed Asifuddin vs State of Andhra Pradesh [2005 CriLJ 4314] - Involved unauthorized tampering of mobile handset software source code.
- Bhimsen Gand vs State of Rajasthan [2006 CriLJ 3643] - Concerned alteration of digital evidence, emphasizing the need to preserve source code integrity.



Section 66 - Computer Related Offences

Covers acts such as dishonestly or fraudulently accessing, downloading, copying, or altering data without permission. Punishable with up to 3 years imprisonment or a fine up to ₹5 lakhs, or both.

- A. Shankar vs State Representative (2010) - The accused was found guilty of unauthorized access and misuse of digital data, reinforcing that fraudulent digital actions are prosecutable under Section 66.

Section 70 - Protected Systems

Covers unauthorized access to "protected systems" declared by the government. Only authorized personnel may access these systems.

Example: A petitioner was found to have unauthorizedly accessed the protected system of legal advisors, violating this section.



Section 66A - Punishment for Sending Offensive Messages via Communication Services

Criminalized sending offensive, false, or threatening electronic messages intended to cause annoyance, inconvenience, or insult. Punishable with up to 3 years imprisonment and a fine.

Landmark Judgment:

- Shreya Singhal vs Union of India (2015) The Supreme Court struck down Section 66A as unconstitutional, ruling it violated the right to freedom of speech and expression (Article 19(1)(a)) due to its vague and overly broad language, leading to misuse and chilling effects on free speech.

Section 66A - Sending Offensive Messages through Communication Services

- **Struck Down:** *Shreya Singhal vs Union of India* (2015)
- Declared **unconstitutional** for violating **Article 19(1)(a)** (freedom of speech) and **not protected under Article 19(2)** (reasonable restrictions).
- Struck down in its **entirety** due to vagueness and potential for misuse.

Section 69A - Power to Block Public Access to Information

- Accompanied by the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.
- **Held constitutionally valid** by the Supreme Court in *Shreya Singhal*, given the due process and safeguards prescribed in the Rules.

Section 79 - Intermediary Liability

- Recognized as **valid**, but **Section 79(3)(b)** was **read down** to mean that intermediaries can only be held liable if they fail to act on **actual knowledge** received through a court order or appropriate government notification.



Section 67 - Publishing/Transmitting Obscene Material in Electronic Form

- **Punishment:** Imprisonment up to 3 years and fine for first conviction.
- **Key Case:** *Avnish Bajaj vs State (2005)* (Bazee.com case)
 - The then CEO of Bazee.com was arrested under Section 67 for an obscene video listed for sale on the platform.
 - Though he demonstrated due diligence, the I.T. Act at that time did **not define or protect intermediaries**, leading to his arrest.
 - This case later influenced the **inclusion of intermediary provisions** in the amended IT Act (2008).



Sharat Babu Digannath vs Govt. of NCT of Delhi

- The petitioner, **Sharat Babu Digannath**, was serving as **Senior Manager, Trust & Safety at Baazee.com (BIPL)** when the controversial **DPS MMS clip** was listed for sale on the platform.
- His role involved ensuring portal safety, acting on reported violations, and blocking or removing inappropriate content or users.

Court's Finding:

- Although the petitioner was **discharged from charges under Section 67 r/w 85 of the IT Act and Section 294 IPC**,
- The court found **prima facie sufficient material to proceed** against him under **Section 292 IPC** (obscenity in books, etc.), citing his functional responsibility over content moderation and safety.

Section 79 - Exemption of Liability for Intermediaries

- Provides conditional immunity to intermediaries (e.g., online platforms) from liability for third-party content, subject to due diligence and compliance with the Information Technology (Intermediary Guidelines) Rules, 2011.
- **Key Case:** Christian Louboutin SAS vs Nakul Bajaj & Others (Nov 2018)
 - Great analysis of Sec 79 of I.T Act 2000 and the intermediary guidelines done by Hon'ble Justice Prathiba M. Singh.
 - The judgment clearly outlines the circumstances under which an intermediary may be deemed to be **abetting the sale of online products or services**, thereby losing the exemption from liability.
 - In this case, the **complainant**, a luxury shoe manufacturer, filed for an injunction against the e-commerce portal www.darveys.com for alleged **trademark infringement**, in collaboration with sellers of counterfeit goods.



Kent RO Systems Ltd. vs Amit Kotak & Others (E-Bay Case, Jan 2017)

- A landmark case in India addressing the consultative society of sec 66 A of I.T. Act 2000. Although not directly about **Section 66A**, this case contributes to the evolving legal framework around **intermediary liability and online content regulation** in India.
- The Supreme Court submitted the provisions after two persons were arrested in Palghar Mumbai for allegedly operating offensive comments on Facebook about the shutdown of Mumbai faking the death of political leader.
- The case raised critical questions about the **balance between free speech and content regulation**.
- The Supreme Court eventually struck down Section 66A ruling that it violated the right to freedom and speech and expression enshrined under Act 19 (1) (a) if the Constitution of India.
- The Indian judiciary has made significant strides in interpreting and applying legal principles in cybercrime cases, as evident in judgments such as **State of Punjab, U.S. vs Thomas, Rambabu Saxena, and Shreya Singhal vs Union of India**.



Conclusion

The judiciary, through the interpretation of various statutes, is progressively adapting **traditional legal principles to the digital age**.

This evolving jurisprudence reflects a **comprehensive approach** to address the complex and dynamic nature of cybercrime.

By aligning legal reasoning with technological realities, the judiciary plays a pivotal role in **combating digital frauds** and ensuring justice in the cyberspace era.



Thank You

