Cross-Border Cyber Offences and Jurisdictional Challenges in Global Cyber Investigations – With Special Reference to Indian Law and Case Studies

Author- Shreyashi Dubey (Research scholar, Deen Dayal Upadhyay University, Gorakhpur)

Co- author – Dr. Ashish Shukla (Asst. Professor, Deen Dayal Upadhyay University, Gorakhpur)

Abstract

In an era of borderless digital communication and global data exchange, cyber offences have evolved into transnational phenomena that challenge conventional notions of sovereignty and jurisdiction. India, as one of the world's largest digital ecosystems, faces complex legal and investigative challenges in addressing cross-border cybercrimes such as hacking, online fraud, identity theft, and data breaches. While the Information Technology Act, 2000 (IT Act) extends jurisdiction beyond India's physical boundaries.

The practical enforcement of such jurisdiction remains fraught with limitations in international cooperation, mutual legal assistance, and evidence acquisition. This paper critically examines the jurisdictional challenges . India faces global cyber investigations, analysing doctrinal approaches such as territoriality, nationality, and the effects principle. It also explores how Indian courts and law enforcement agencies interpret these doctrines in cyber contexts. Through the lens of Indian statutes and landmark cases like Suhas Katti v. Tamil Nadu (2004), Shreya Singhal v. Union of India (2015), and CBI v. Arif Azim (2008), the paper discusses the operational gaps between law and practice. Comparative insights from international frameworks such as the Budapest Convention and the U.S. CLOUD Act are considered to evaluate India's strategic position in global cyber governance. Finally, the study proposes reforms to strengthen India's cross-border investigative capabilities, harmonize its cyber laws with international standards, and ensure a balance between state sovereignty, privacy, and global digital security.

Introduction

Cybercrime is no longer confined to geographical borders. The interconnected nature of digital technologies has enabled perpetrators to operate remotely from any part of the world, making jurisdictional boundaries increasingly porous. According to international agencies, a significant portion of cyber incidents reported in the Asia-Pacific region have cross-border components (Interpol, 2023). In India, the digital economy's rapid growth—bolstered by initiatives like Digital India—has resulted in unprecedented vulnerabilities to such offences. The complexity of cross-border cyber offences stems from their multidimensional nature:

while the act (such as data theft or phishing) may occur in one jurisdiction, the effects (like financial loss or data compromise) are often felt elsewhere. This raises fundamental questions: under what conditions can Indian courts and investigative agencies claim jurisdiction? How can they collect admissible evidence when servers, perpetrators, or victims are in different countries? What international mechanisms can India use to cooperate effectively in such cases? This paper provides a comprehensive analysis of these issues by examining Indian laws and case studies in relation to global frameworks. It identifies critical gaps between legislative intent and operational execution and offers recommendations to bridge these divides.

Concept of Cross-Border Cyber Offences

Cross-border cyber offences refer to illegal digital activities that either originate, transit through, or impact multiple jurisdictions. Common categories include hacking, ransomware, phishing, financial fraud, child exploitation, and online defamation. The defining feature of such offences is the transnational element—either the offender, victim, or the digital infrastructure involved spans more than one country (UNODC, 2021). In India, cyber offences are defined primarily under Chapter XI of the Information Technology Act, 2000. Section 66 deals with computer-related offences, while Sections 66C and 66D cover identity theft and cheating by personation. Section 67 penalizes the transmission of obscene or sexually explicit content, which often involves cross-border publication or hosting on foreign servers. The digital ecosystem's borderless nature often obscures the locus delicti (place of offence). For instance, a hacker in Singapore could target a financial institution in Mumbai using servers located in Germany. Determining which country has jurisdiction in such scenarios becomes a matter of international law, diplomatic negotiation, and mutual legal assistance .Two key challenges arise in defining jurisdiction over cyber offences: (1) multiplicity of jurisdictions, where acts and effects occur in different countries; and (2) absence of harmonized definitions, as different jurisdictions may classify and penalize cybercrimes differently, complicating prosecution.

Jurisdictional Doctrines and Principles

Jurisdiction forms the cornerstone of criminal law enforcement. In cyber offences, where actions, servers, and effects are scattered across multiple territories, determining which court or authority can exercise jurisdiction becomes particularly intricate. The traditional doctrines of territoriality, nationality, protective principle, and effects principle are all invoked to address cyber incidents with transnational dimensions. The principle of territoriality posits that a state has the right

to exercise legal authority over acts committed within its geographical boundaries. India codifies this in Section 2 of the CrPC and Section 3 of the IPC. However, Section 1(2) and Section 75 of the IT Act explicitly extend the law's application to offences or contraventions committed outside India if the act involves a computer, system, or network located in India. Under the nationality principle, a state may claim jurisdiction based on the offender's

citizenship, and the passive personality principle allows jurisdiction based on the victim's nationality. India incorporates aspects of both principles in Section 4 of the IPC and Section 4(3) of the BNS. The effects doctrine extends jurisdiction to foreign conduct that produces harmful effects within a nation's borders.

Indian Legal Framework for Cross-Border Cyber Offences

India's cybercrime regulation operates through a combination of statutory instruments, procedural codes, and sectoral guidelines. The principal framework includes the Information Technology Act, 2000 (IT Act), the Bharatiya Nyaya Sanhita, 2023 (BNS), the CrPC, and evidentiary provisions under the Indian Evidence Act, 1872. The IT Act's Sections 43 and 66 define unauthorized access, hacking, and data theft. Sections 66C and 66D criminalize identity theft and impersonation; Section 67 prohibits obscene digital content. Section 75 establishes extraterritorial jurisdiction when Indian computer systems or networks are involved; Section 78 empowers police officers to investigate offences under the Act. The BNS modernizes substantive offences and extends jurisdictional reach through provisions such as Section 4(3). Procedurally, Section 65B of the Evidence Act governs admissibility of electronic records, requiring certification for authenticity. The Supreme Court's decisions **in Anvar P.V. v. P.K. Basheer (2014) and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)** clarified evidentiary requirements, making cross-border evidence collection more exacting. Data protection (Digital Personal Data Protection Act, 2023) introduces constraints on cross-border transfer of personal data, which impacts international cooperation when foreign authorities seek Indian user data for cybercrime investigations (Chatterjee, 2024).

Case Law Analysis: Indian and Comparative Perspectives

Judicial precedents play a critical role in interpreting the scope of jurisdictional and procedural powers in cybercrime cases. In India, statutory provisions like Section 75 of the IT Act provide the legislative foundation for extraterritorial jurisdiction, but courts have often had to innovate to apply traditional doctrines to digital realities. Key Indian cases include-

1) **Suhas Katti v. State of Tamil Nadu (2004)**, where postings hosted on foreign servers resulted in conviction because the harm was felt within India.

2) **CBI v. Arif Azim (2008)**, which affirmed that unauthorized access originating in India can ground jurisdiction even if victims were abroad.

3) Shreya Singhal v. Union of India (2015), which struck down Section 66A and underscored constitutional safeguards in digital regulation. The Supreme Court delivered a unanimous judgement declaring **Section 66A of the Information Technology Act, 2000** unconstitutional.

Practical investigative barriers frequently undermine India's statutory jurisdiction. First, evidence location and preservation present technical obstacles: logs, ephemeral messages, and

snapshot data are often volatile and may be overwritten before foreign cooperation is secured. Mutual Legal Assistance Treaties (MLATs) serve as the standard formal channel for cross-border evidence requests, but they are routinely slow and bureaucratic . Second, conflicting legal frameworks—data
protection regimes, privacy safeguards, and intermediary liability rules—create legal friction. For example, EU data protection standards post-Schrems II raise higher scrutiny for transfers; India's DPDP imposes local restrictions that may require judicial authorization before transfer. Third, encryption and end-to-end secured platforms prevent meaningful access to content even if jurisdiction is established. Law enforcement's inability to compel decryption in the absence of keys remains a practical misfortune. Fourth, platform and intermediary cooperation is inconsistent. Global platforms may respond only to domestic court orders or MLATs, and their transparency reports show wide variation in compliance (Google Transparency Report, 2024). Fifth, extradition and prosecution are hampered by political factors, lack of bilateral treaties, and differing criminalization of cyber conduct.

Policy Recommendations

To enhance India's capacity to investigate and prosecute cross-border cyber offences, the following policy measures are recommended: 1. Accede to multilateral frameworks or negotiate equivalent regional agreements: India should consider joining the Budapest Convention or negotiating interoperable regional instruments promoting expedited preservation, mutual assistance, and standardized procedures for electronic evidence (UNODC, 2021). 2. Establish a domestic expedited preservation regime: Amend procedural law to enable courts to issue time-bound preservation orders that can be communicated to foreign providers through diplomatic channels or via direct provider liaison. 3. Expand MLA efficiency and digitalize MLAT processing: Invest in digital platforms to file, track, and process MLAT requests, reducing administrative delay. Introduce statutory timelines and monitoring for responses. 4. Negotiate bilateral executive agreements with major cloud-hosting jurisdictions:

Conclusion

Cross-border cyber offences present a complex challenge that straddles law, technology, and international relations. India's statutory framework—anchored by the IT Act and supplemented by modern statutes like the BNS and DPDP—provides legal bases for asserting extraterritorial jurisdiction. Judicial precedents have, by and large, endorsed an effects-based and nexus-driven approach, enabling India to prosecute offences that have material impact within its territory. Nonetheless, statutory jurisdiction alone cannot guarantee successful enforcement. Practical obstacles—slow mutual legal assistance, data protection conflicts, encryption, and platform non-cooperation—continue to frustrate investigators. Comparative models such as the CLOUD Act and Budapest Convention offer useful tools, but India must adapt them to its constitutional and policy priorities. A balanced strategy that combines legal

reform, international agreements, procedural modernization, and robust safeguards for privacy and civil liberties is necessary. Through proactive diplomacy, technological investment, and clear legal frameworks, India can strengthen its ability to respond to cross-border cyber offences while maintaining the rule of law and protecting citizens rights.

References

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 12 SCC 1.

Bhatia, R. (2022). Challenges in Mutual Legal Assistance for Cybercrime. Journal of Cyber Law, 7(2), 45-62.

Chatterjee, S. (2024). Data Protection and Cross-Border Evidence: India's Legal Dilemma. Indian Journal of Law and Technology, 2(1), 15-33.

Digital Personal Data Protection Act, 2023, Government of India.

Gupta, A. (2021). Locus Delicti in Cyber Offences. Law & Policy Review, 14(3), 101-128. Interpol. (2023). Cybercrime in the Asia-Pacific: Trends and Responses.
Joshi, M. (2023). CLOUD Act and Global Data Access: Implications for India. International Journal of Cyber Policy, 5(1), 22-39.

Kaur, P. (2021). Encryption and Investigations: Technical Barriers to Cybercrime Prosecution. Cybersecurity Bulletin, 3(4), 9-27.

Kumar, S. (2018). Extraterritorial Jurisdiction in Indian Cyber Law. Delhi Law Review, 12(2), 77-98. Mehta, R. (2022). Territoriality in Cyber Law. National Law Journal, 9(1), 55-73.
Microsoft Corp. v. United States, 584 U.S. ___(2018).

Rao, N. (2021). Jurisdiction over Online Content: Indian Courts and Foreign Servers. Media Law Journal, 6(2), 34-50.

Reddy, L. (2023). India and the Budapest Convention: Policy Considerations. International Law Quarterly, 11(3), 88-110.

Schrems II, Case C-311/18, Court of Justice of the European Union (2020). Shreya Singhal v. Union of India, (2015) 5 SCC 1.
Suhas Katti v. State of Tamil Nadu, Crl.O.P. No. 10479 of 2003 (Madras High Court, 2004).

Tiwari, P. (2022). Cybersecurity Governance in India. Journal of International Affairs, 18(4), 200-219. UNODC. (2021). Comprehensive Study on Cybercrime.
U.S. v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001). Information Technology Act, 2000, Government of India. Bharatiya Nyaya Sanhita, 2023, Government of India. Code of Criminal Procedure, 1973, Government of India. Indian Evidence Act, 1872, Government of India.