JURISDICTION IN CYBERSPACE: EVALUATING THE CAPACITY OF INDIAN COURTS TO RESPOND TO TRANSNATIONAL CYBERCRIME

Jurisdiction, a cornerstone of legal authority, traditionally derives its legitimacy from well-defined territorial boundaries. Courts have long exercised power based on geographic proximity over persons, property, and subject matter located within their designated regions. However, the emergence of cyberspace has radically disrupted these foundational principles. The internet's inherently borderless nature allows individuals and entities to act across multiple jurisdictions simultaneously, often without physical presence in any of them. This fluidity challenges the conventional application of territorial, personal, and subject-matter jurisdiction and raises complex legal questions about enforceability and accountability in digital environments[1].

It could be noted that, a single online transaction or publication can instantly affect users across continents, making it difficult to determine the appropriate legal forum. Courts have attempted to adapt by developing new jurisdictional tests, such as the "effects doctrine" and "purposeful availment," to address the complexities of online interactions. Notably, in *Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy*[2], the Delhi High Court emphasised that mere accessibility of a website is insufficient to establish jurisdiction; there must be an intentional targeting of users within the forum state. Similarly, scholars such as Jack Goldsmith and Tim Wu argue that despite the internet's global reach, sovereign states continue to assert control through evolving jurisdictional claims[3].

This paper seeks to examine the tension between traditional jurisdictional doctrines and the realities of cyberspace, exploring how courts and legal systems are redefining boundaries in an increasingly digital world.

The Problem of Borderlessness

One of the most pressing challenges is that cybercrimes often originate in one country, affect individuals or systems in another, and may involve infrastructure in a third. For instance, an Indian citizen might be defrauded by an accused sitting in Russia, using servers located in

[1] Calder v. Jones, 465 U.S. 783 (1984).
[2] Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy, 2008 SCC OnLine Del 379.
[3] Goldsmith, Jack, and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press, 2006.

Singapore. Under these conditions, questions arise about where the offence took place and which court can take cognisance of the case.

Difficulty in Applying Territorial Jurisdiction

Sections 210 to 212 of the Bharatiya Nagarik Suraksha, 2023 deal with jurisdiction in criminal matters, largely based on where the offence occurred or where its consequences were felt. However, in cyberspace, the "place of occurrence" is often abstract or diffused. Courts and investigators struggle to pin down an exact location, particularly when perpetrators use VPNs, proxy servers, or dark web technologies to mask their origins.

In India, Section 75 of the IT Act, 2000[4]tries to address this by granting the Act extraterritorial reach. It states that the Act applies to any offence or contravention committed outside India if it involves a computer, system, or network located in India. While this provision appears powerful on paper, its practical enforcement is limited by the need for international cooperation, which is often slow or unavailable.

Lack of Consistency in Judicial Interpretation

Indian courts have not yet adopted a clear and consistent test for asserting jurisdiction in cyber matters. In some cases, courts have proceeded based on the location of the victim or the impact of the offence, while in others they have relied on the physical location of the accused or digital evidence. This inconsistency creates uncertainty for both litigants and law enforcement agencies.

For instance, in *Swami Ramdev v. Facebook Inc*[5]., the Delhi High Court applied a form of "global injunction" to content posted online, ordering its removal not just within India but worldwide. While this was seen as a bold assertion of judicial reach, it also raised concerns about overreach and enforceability. In contrast, the Court in *MF Hussain v. Raj Kumar Pandey* rejected jurisdiction merely because offensive content was accessible in India. Similarly, *Banyan Tree Holdings v. A. Murali Krishna Reddy* rightly applied the targeting and purposeful availment test, but this standard has not been uniformly adopted across Indian courts. This doctrinal inconsistency leads to unpredictability, making it difficult for complainants and enforcement agencies to confidently assess whether a particular forum will accept jurisdiction in a given cyber offence.

[4] Information Technology Act, 2000, § 75, No. 21, Acts of Parliament, 2000 (India).
[5] *Swami Ramdev & Anr. v. Facebook, Inc. & Ors.*, (2019 SCC OnLine Del 10701).

Challenges in Investigations and Enforcement

Even when jurisdiction is theoretically established, the practical challenges of gathering evidence from foreign jurisdictions remain a significant obstacle in cyberspace-related cases. Indian authorities often rely on Mutual Legal Assistance Treaties (MLATs)[6] to request evidence from other countries. However, these agreements can be slow, cumbersome, and subject to the discretion of the foreign jurisdictions involved, which may not always honour such requests in a timely or consistent manner. This issue is particularly pronounced in cases involving major tech corporations such as Google, Meta, and Twitter, where even basic subscriber data or server logs can take months to retrieve, if they are obtained at all. Further complicating matters is India's non-membership in the Budapest Convention[7], the only major international treaty addressing cybercrime. This absence limits India's access to real-time cooperation mechanisms and information-sharing platforms, which could expedite the process of securing evidence across borders. As cybercrime cases grow more complex and international in scope, the legal framework for cross-border cooperation remains a major bottleneck in delivering justice, especially for countries like India, which do not have robust real-time mechanisms for digital evidence exchange.

Jurisdiction forms the backbone of any criminal justice system, determining the authority of courts to adjudicate a matter. In the context of cyberspace, where activities are delinked from physical geography, traditional jurisdictional doctrines face serious limitations.

Section 75, Information Technology Act, 2000

Section 75 is India's principal statutory attempt to address the borderless nature of cybercrime. It reads:

"*This Act shall apply also to any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India."*

This provision gives the IT Act extraterritorial reach; however, in the absence of detailed procedural rules or supporting bilateral/multilateral enforcement mechanisms, its applicability

[6] *U.S. v. Microsoft Corp*., 138 S. Ct. 1186 (2018).
[7] Convention on Cybercrime (Budapest Convention), 2001 – The only binding international treaty aimed at addressing Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.

remains largely symbolic. There is also no settled jurisprudence that definitively interprets Section 75 in practical terms, leaving both courts and enforcement agencies in a grey area.

Section 1(5), Bhartiya Nyaya Sanhita, 2023

Section 1(5) BNS provides:

(5) The provisions of this Sanhita shall also apply to any offence committed by— (a) any citizen of India in any place without and beyond India; (b) any person on any ship or aircraft registered in India wherever it may be; (c) any person in any place without and beyond India committing offence targeting a computer resource located in India.

Although clause (5) supports the IT Act's extraterritorial objectives, the BNS remains largely offence-specific, and jurisdiction under this provision is only enforceable if procedural hurdles under the BNSS are satisfied.

Sections 197 to 209, Bharatiya Nagarik Surakha Sanhita, 2023

Sections 197 to 209 BNSS establish the general rule that offences shall be tried where they are committed. However, in cases involving cybercrime, determining the *locus delicti* (place of offence) is complicated by VPNs, masked IP addresses, and remote execution of acts.

Section 208 of BNSS further provides for the trial of offences committed outside India, but only with prior sanction from the Central Government, adding yet another procedural bottleneck.

Indian courts have increasingly encountered cases where cyber activity implicates multiple jurisdictions. In response, they have looked to international doctrines such as effects-based jurisdiction and the targeting test to determine when Indian jurisdiction is appropriate.

1. **Effects Doctrine – *Swami Ramdev v. Facebook Inc*[8].** In this landmark judgment, the Delhi High Court issued a global takedown order against defamatory content, holding that if the impact of the online act is felt in India, the Indian courts can exercise jurisdiction. The Court drew on the effects doctrine, asserting that territorial impact suffices to establish jurisdiction, even when the platform is headquartered abroad.
2. ***Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy,***[9] this case is widely recognised as the first authoritative Indian precedent adopting the U.S.-based **"Zippo Sliding**

[8] *Supra* Note 3
[9] *Supra* Note 2.

Scale" test. The Delhi High Court held that mere accessibility of a foreign website in India does not confer jurisdiction. Instead, the defendant must have **purposefully directed activity toward India**, such that they avail themselves of the benefits and protections of Indian law.

3. **Targeting Test – *WWE v. Reshma Collection,***[10] the Court held that offering goods or services specifically targeting Indian consumers via an interactive website was sufficient to establish jurisdiction. This case endorsed the "targeting test", stating that the focus should be on whether the alleged infringing content or act was intended for Indian users.

4. **Judicial Conservatism – *MF Hussain v. Raj Kumar Pandey*** [11] the Delhi High Court refused to entertain a complaint against an artist for allegedly obscene digital content hosted abroad, holding that jurisdiction cannot be presumed merely because the content is accessible in India. This reflects a more cautious judicial approach, particularly when global artistic or expressive rights are implicated.

5. **Early Recognition – *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra,*[12] India's first reported cyber defamation case**. The Delhi High Court, without much discussion on technical jurisdictional tests, issued an injunction against defamatory emails, holding that damage caused to reputation within India was sufficient to assume jurisdiction. Although fact-specific, this case reflected an early recognition of cross-border implications of digital acts.

Indian courts do not yet follow a uniform test for jurisdiction in cyber matters. While some judgments, such as *Swami Ramdev* and *WWE*, apply an effects- or targeting-based approach, others (like *MF Hussain*) adopt a more restrictive view. This lack of doctrinal consistency poses a serious challenge to predictability and legal certainty in cybercrime litigation. Courts often rely on territorial concepts under the CrPC, now BNSS, which are designed for conventional crimes and are ill-suited to address transnational, decentralised cyber offences. The absence of procedural guidelines for implementing Section 75 of the IT Act exacerbates this problem.

Despite legislative intent, India's cyber jurisdiction framework lags behind international best practices in terms of creating operational and enforceable rules for cross-border digital activities. The comparative models of jurisdictions like the EU and U.K. show that effective jurisdiction over cross-border cyber offences requires harmonisation, cooperation, and procedural innovation[13]. India must prioritize these objectives by creating clear statutory

[10] *WWE v. Reshma Collection* 2014 SCC Online Del 1882.
[11] *Maqbool Fida Husain v. Raj Kumar Pandey*, 2008 Cri. L.J. 4107 (Del. HC).
[12] *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra*, Suit No. 1279/2001, Delhi District Court (Feb. 12, 2014).
[13] Narayan, S., & Choudhury, S. (2020). *Cyberspace Sovereignty: A Comparative Analysis of India's Legal Framework on Cyber Jurisdiction*. National Law School Journal, 45(2), 124-151.

frameworks, improving cooperation mechanisms, and engaging with international treaties to strengthen its cyberspace sovereignty and better safeguard its digital environment[14].

Section 75 of the Information Technology Act, 2000, was designed to give the law extraterritorial application. However, its real-world utility remains limited by a lack of enabling procedural law. For instance, neither the BNSS nor the IT Act Rules specify:

- How summons or warrants are to be executed abroad;
- What evidentiary standard applies when the accused is a foreign national?
- Whether jurisdiction can be asserted in the absence of bilateral cooperation.

This renders Section 75 more aspirational than enforceable. Even though Section 1(5) of the BNS and Sections 197-209 of the BNSS theoretically support extra-territorial jurisdiction, these provisions were not designed with cyberspace in mind and require central government sanction or diplomatic channels, thereby delaying justice.

Indian investigative authorities face practical hurdles in establishing and exercising jurisdiction in cyber offences:

- **Reliance on MLATs** (Mutual Legal Assistance Treaties) leads to prolonged delays, with requests for digital evidence taking months to materialise, if at all.
- **Law enforcement lacks real-time cooperation protocols** with major global intermediaries such as Meta, Google, or Twitter.
- **Digital forensics capabilities** are not uniformly distributed across states; specialised knowledge is limited to certain central agencies like CERT-In or the CBI cyber units.
- **Trial courts often lack technical training**, resulting in erroneous admissibility rulings.

Jurisdictions such as the United States and the European Union have developed clearer judicial standards for asserting cyber jurisdiction. The effects doctrine, targeting test, and Zippo sliding scale have become embedded in their case law.

[14] De Zwart, M., & Binns, R. (2016). *Cross-Border Data Requests and Privacy in the Age of Global Surveillance: How the EU and U.S. Regulate the Cyber Landscape*. International Journal of Law and Information Technology, 24(4), 329-358.

In the U.S., courts evaluate whether a website is interactive, passive, or commercial (Zippo Mfg. Co. v. Zippo Dot Com, Inc., while the *Calder v. Jones* doctrine allows jurisdiction when the intentional act is aimed at the forum and causes harm.

The EU, through the Brussels I Recast Regulation and the GDPR, ensures that any platform targeting EU citizens must submit to its jurisdiction. Even outside the EU, companies must comply with GDPR if they process data of EU residents, signifying robust extraterritorial intent backed by enforceable frameworks. By contrast, India's attempts at jurisdiction in cybercrime cases appear case-specific rather than principle-driven and suffer from a lack of procedural coherence. India's non-signatory status to the Budapest Convention on Cybercrime further isolates it from real-time investigative cooperation frameworks. While concerns about sovereignty and unequal treaty formation are valid, they must be weighed against the operational cost of relying solely on outdated bilateral agreements. Most nations with active cybercrime prosecution mechanisms are either signatories to the Budapest Convention or have dedicated mutual legal cooperation frameworks. India, in contrast, often navigates jurisdictional assertions through outdated diplomatic channels, limiting its responsiveness in cybercrime matters.

Even domestically, the lack of a model cyber jurisdiction framework has led to inconsistent policy enforcement. India has yet to formalise judicial or statutory adoption of a test, such as the targeting test, to determine jurisdictional reach. The Indian legal system is not inherently incapable of asserting cyber jurisdiction unless supported by coherent rules and proactive institutional responses. India's jurisdictional assertions in cyberspace will remain legally sound but practically unenforceable.

Cyber jurisdiction challenges lie at the intersection of constitutional due process, technological neutrality, and international comity. Indian law demonstrates an intent to regulate this space but falls short in procedural readiness and institutional infrastructure. The convergence of government policy recommendations, judicial guidance, and international norms presents an urgent call for harmonised reform.

Rather than reinventing jurisdictional principles, India must implement existing global standards within a contextualised domestic framework. In an era where digital borders blur faster than law can adapt, jurisdiction must evolve as a principle of both authority and cooperation, anchored in constitutional values and committed to cyber justice.