AN ANALYTICAL STUDY ON CYBERSPACE JURISDICTION: LEGAL FRAMEWORK AND CHALLENGES

Sufia Sheikh, Asst. Professor of Law, Indian Institute of Legal Studies

ABSTRACT

Cyberspace and the internet have become essential to human existence. Every aspect of our life has been significantly impacted by the internet, including business, education, globalisation, developing global connections through social media, politics, healthcare, infrastructure, research, and technology. Cyberspace is the virtual world created with the help of the internet and computers. Cyberspace encompasses all electronic devices that operate via the internet. These include software, data storage devices, websites, emails, the internet, mobile phones, and even automated teller machines. As the evolution of the internet has assisted in building network and connectivity in this global world it has also aided in the emergence of internet related crimes and incidental issues related therewith. The ability to ascertain the location of the crime and to hear a specific case that will be heard in a suitable court of law is known as jurisdiction. The foundation of traditional legal systems is territorial jurisdiction, which states that the law only applies inside a certain jurisdiction's borders. However, because the internet is worldwide and linked, it becomes challenging to establish distinct geographical boundaries in cyberspace. Because cyberspace has no borders, it is unclear which jurisdiction should have the power to control and enforce laws pertaining to online activity. Two different countries' laws may be involved in a single online transaction. Generally, where the cause of action occurs is typically the jurisdiction. However, when there are numerous parties involved from all over the world, the process of establishing jurisdiction has become extremely challenging. This research paper attempts to explain the concept, types, theories relevant for determination of Jurisdiction in Cyberspace and existing legal framework through national and international perspectives to combat Cyberspace Jurisdictional challenges.

Keywords: Cyberspace, Cyber Jurisdiction, Theories, Legal Framework, Challenges

CHAPTER 1. INTRODUCTION

Despite the establishment of various tests to determine cyberspace jurisdiction, it remains a contentious issue in legal courts when dealing with cybercrime cases that involve multiple countries. Different nations use different criteria to determine jurisdiction, meaning a jurisdictional test that is valid in one country may not be in another.[1] Consequently, when the parties involved are from different nations, it becomes highly challenging to determine which country's jurisdiction should apply. In such cases, it may be necessary to apply multiple tests to establish jurisdiction. In India, while the Information Technology Act of 2000 regulates cyberspace, it does not address territorial jurisdiction. Therefore, it is essential for lawmakers to introduce provisions that address extra-territorial jurisdiction within the Act. Given the rapid increase in global internet usage, laws must evolve to effectively address cybercrime and jurisdictional issues. International law should set clear parameters for determining jurisdiction, and in cases where jurisdiction remains unclear, such matters should be handled by the International Court of Justice.

1.1 Essential for enforcement of valid Jurisdiction in Cyberspace:

Prescriptive Jurisdiction: It allows a country to establish laws that govern a person's activities, status, circumstances, or choices, regardless of the person's nationality or the location where the act occurred. This type of jurisdiction is unlimited, meaning a country has the authority to pass laws on any subject. However, international law restricts any nation from enacting laws that contradict the interests of other countries.

Jurisdiction to Adjudicate: It gives a state the authority to resolve civil or criminal matters involving an individual, even if the state itself is not a party to the case. A mere connection between the state and the individual is enough to establish jurisdiction. It is important to note that having prescriptive jurisdiction does not automatically grant a state the jurisdiction to adjudicate.

Jurisdiction to Enforce: It is dependent on the existence of prescriptive jurisdiction. If a state lacks prescriptive jurisdiction over an individual or action, it cannot enforce its laws to punish

[1] David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1375 (1996) (noting the territorial variance in jurisdictional frameworks applied to internet activities).

violations. Moreover, this jurisdiction is not absolute; a state cannot enforce its laws on an individual or crime that takes place in another country.

CHAPTER-II: Tests to determine Country's Jurisdiction in International Law:

1. **Minimum Contacts Theory**: The Minimum Contact theory applies when one or both parties involved are outside the territorial jurisdiction of the Court. It is used to determine the Court's authority over the parties by assessing the nature and extent of their interactions, such as services or transactions with the Forum State. According to the minimum contact rule, if a corporation has some level of presence or contact within the state where the Lawsuit is filed, it is subject to that state's law and can be sued in that state's court. Examples of minimum contact rule include operating a business in the state, being incorporated there or making visits to the state. The theory was established in the landmark case of *International Shoe Co. v. Washington*,[2] In this significant decision, the U.S. The Supreme Court ruled that a party, especially a corporation, can be subject to the jurisdiction of a state court if it has "minimum contacts" with that state. This ruling has important implications for corporations engaged in interstate commerce. The Court determined that a lawsuit cannot be filed against an individual unless they have minimum contacts with the forum state.

After *International Shoe case*, courts typically use a three-part test to assess whether minimum contacts are sufficient for establishing jurisdiction:

1. The non-resident defendant must engage in some action or transaction with the forum state or purposefully avail themselves of the privilege to conduct activities within the state, thereby enjoying its benefits and protections.

2. The claim must stem from or be connected to the defendant's activities within the forum state.

3. The exercise of jurisdiction must be deemed reasonable.

2. Calder Effect Test: The Effect test requires certain conditions to be met, primarily that the defendant's actions are directed specifically at the forum state with the

[2] 326 U.S. 310 (1945)

knowledge and intent to cause harm to it. If the court determines that the defendant's actions have caused injury to the forum state, personal jurisdiction in cyberspace cases can be asserted, even when there is no direct contact with the state. The theory was established in the landmark case *Calder v. Jones*, 465 U.S. 783 (1984), where the U.S. Supreme Court ruled that a court in one state could assert personal jurisdiction over the author and editor of a national magazine that published a defamatory article about a resident of that state, especially when the magazine had wide circulation in that state. The Court held that personal jurisdiction could be asserted over the author or editor of a libellous article if they knew the article would be widely distributed in the state and harm the person it was about. In this case, the Court determined that California courts had jurisdiction over the defendants.

3. Personal Jurisdiction Theory: This theory states that all individuals residing within a defined area fall under the jurisdiction of the relevant court. However, issues arise when one or more parties involved in a dispute are located outside of that jurisdiction, or even outside the specific political entity or country. This concept faces challenges in the realm of the internet, where numerous cases, both civil and criminal, involve parties or defendants from different countries. The traditional theory was modified in the case of *Zippo Manufacturing Co. v. Zippo Dot Com Inc*[3]., which introduced the "sliding scale" theory. This theory suggests that the nature of the defendant's activity is the key factor in determining jurisdiction, and that passive websites do not create personal jurisdiction.

4. The "sliding scale" or "Zippo" Test: This theory is widely recognized as the standard used by Federal Courts to determine personal jurisdiction in internet-related cases. These cases are typically decided by evaluating the website's "interactivity." Courts have ruled that the more commercial and interactive a website is, the more likely it is that the website operator has "purposefully availed itself" of the jurisdiction of the forum state.

5. Country-of -origin or Country of destination theory: There are differing views on the applicability of the country-of-destination rules for online commercial activities, as businesses may be required to respond to legal actions in a court located hundreds of

[3] 952 F. Supp. 1119 (W.D. Pa. 1997).

miles away for failing to comply with the laws of that country. This situation could make it not only impractical for entrepreneurs to conduct business in such a manner, but it would also impose additional costs for handling litigation outside their own jurisdiction.

6. Forum Selection Theory: Under the Forum Selection Theory, parties may agree in advance to resolve their disputes in a specific court, either within a natural jurisdiction or by selecting a foreign court as a neutral forum, governed by that court's laws. This allows a party to choose the jurisdiction of a competent court for the resolution of their dispute. In other words, if multiple courts have jurisdiction over a matter, the parties are free to select any one of those courts to settle their dispute. If the parties mutually agree that their case will be heard only by one particular court, they must file the suit exclusively in that court.

CHAPTER III - INTERNATIONAL CONVENTIONS ON CYBERSPACE JURISDICTION:

1. The Convention on Cybercrime also known as Budapest Convention, 2001: It is the first international treaty to address issues related to the Internet and cybercrime, focusing on harmonizing national laws, enhancing cooperation between countries, and improving investigative techniques. The Convention was opened for signatures in Budapest on November 23, 2001, and was signed by the Council of Europe in Strasbourg, France, as well as by countries like Canada, Japan, the Philippines, South Africa, and the United States. However, nations such as India and Brazil initially refused to adopt the Convention, citing their lack of involvement in its drafting. Yet, due to the rising prevalence of cybercrimes, India has been reconsidering its position on the treaty since 2018.

This treaty was the first of its kind to address criminal offenses committed using computer networks, such as the Internet. It covers crimes such as copyright infringement, computer-related fraud, child pornography, and offenses related to cybersecurity. Additionally, the Convention outlines various procedural powers, including the ability to search and intercept materials on computer networks. Its primary goal is to create ‘a common criminal policy aimed at protecting society from cybercrime,’ by encouraging the adoption of relevant laws and fostering international cooperation.

Article 22 of the **Convention on Cyber Crime, 2001** allows a country to claim jurisdiction over a cybercrime if it occurs under the following conditions:

- Within its territory;
- On a ship registered under its flag;
- On an aircraft registered according to its laws;
- By one of its nationals, provided the offense is punishable under the criminal laws of the place where it occurred, or if the offense happens outside the territorial jurisdiction of any state.

India is not yet a signatory to the **CyberCrime Convention**, and the bilateral extradition treaties it has signed with about 50 countries do not explicitly include 'cybercrime' as an extraditable offense.[4]

However, this may not prevent the Indian government from granting extradition. As established in the case of **Ram babu Saxena v. State**[5], even if a treaty does not list a specific offense as extraditable, the Indian government may still approve extradition if the treaty allows for extradition on the basis of a general clause covering additional offenses.

2. The United Nations Convention against Transnational Organized Crime (UNTOC), also known as the Palermo Convention: It was adopted by a UN General Assembly resolution in November 2000. India, as a signatory, joined the convention in 2002. Under this treaty, state parties are required to establish domestic criminal laws targeting organized crime groups and to implement new frameworks for extradition, mutual legal assistance, and cooperation in law enforcement. While the treaty does not specifically address cybercrime, its provisions are still highly applicable. Following this treaty, the Information Technology Act of 2000 was enacted by the Indian Parliament.[6]

---

[4] Helaine Leggat *A new look at the Budapest Convention on Cybercrime* ICTLC (Jan 27, 2025)https://www.ictlc.com/a-new-look-at-the-budapest-convention-on-cybercrime/?lang=en#:~:text=The%20Budapest%20Convention%20is%20a,more%20effective%20and%20subject%20to (last visited Jan 30, 2025).

[5] 1950 A.I.R. 155; 1950 S.C.R. 573 (India).

[6] *UN Convention against Transnational Organized Crime and the Protocols thereto https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html* (last visited Feb 3, 2025).

3. The **Rome Convention**, signed in 1980 by EU Member States, was established to address cross-border consumer contractual disputes. It determines which country's law applies in such disputes. The Convention allows contracting parties the freedom to choose the governing law, stating that 'a contract shall be governed by the law selected by the parties, and this choice must be clear or demonstrated with reasonable certainty.' Additionally, it stipulates that 'the mandatory laws of the consumer's country of habitual residence will always apply, regardless of the chosen law.'[7]

CHAPTER IV - NATIONAL LEGISLATIVE FRAMEWORK TO DETERMINE JURISDICTION IN CYBERSPACE:

1. **Information Technology Act, 2000** acts as the fundamental legislation to regulate electronic communications and related crimes in India. The Information Technology Act, 2000 (IT Act) provides a legal framework to address offences and disputes arising from the use of digital and online platforms. To deal with the borderless nature of cyberspace, the Act incorporates specific provisions to define its jurisdiction.

   Section 1(2) extends the applicability of the Act to the entire country and explicitly includes offences committed outside India, as long as they involve a computer or network located within India.

   Section 75 reinforces this by stating that the Act applies to any offence or breach committed outside Indian territory by any person, regardless of nationality, provided the act involves a computer system situated in India. This grants the Act extraterritorial jurisdiction, crucial for addressing cross-border cybercrimes.

   Section 46 empowers adjudicating officers to resolve certain cyber disputes and contraventions. Jurisdiction is typically based on the location of the affected system or data.

   Section 61 limits the role of civil courts in matters that fall within the jurisdiction of authorities designated under the IT Act, such as adjudicating officers and tribunals.

[7] *Convention on the law applicable to contractual obligations (Rome Convention) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:l33109* (last visited Feb 3, 2025).

2. Bhartiya Nyay Sanhita, 2023

Section 1(5) of BNS covers not only offences within India, but also acts committed abroad by any Indian citizen anywhere, anyone aboard Indian-registered ships or aircraft, or any person (regardless of nationality) who commits an offence against a computer resource in India This enables the law to apply to cyber-offences even when both perpetrator and act originate outside India, so long as the digital target is on Indian soil. Thus, any unauthorized access or attack on infrastructure like servers or data centers in India triggers BNS jurisdiction.

3. Bhartiya Sakshya Adhiniyam, 2023

Section 2(1)(d) defines the term "Document" now explicitly includes digital evidence emails, server logs, website data, locational info, voice and video recordings, cloud content, etc.

Section 2(1)(e) defines the term "Evidence" covers statements given electronically, equating digital testimony with traditional oral evidence.

Section 61 provides equivalence of electronic Records which means electronic or digital records enjoy the same legal validity and enforceability as physical documents provided the conditions mentioned in Section 63 are met.

Section 63-Admissibility Conditions

Admissibility of computer-generated output (e.g., logs or messages) depends on:

a. Regular use of the device in lawful activities,

b. Routine feeding of relevant information,

c. Proper functioning of the device (errors excluded),

d. Output faithfully derived from inputs.

Multiple devices may be treated as a single unit to accommodate modern IT ecosystems. A certificate must accompany electronic evidence, describing how it was produced,

devices involved, and affirming admissibility conditions signed by a responsible person and expert.

CHAPTER V - CHALLENGES AND ISSUES IN CYBERSPACE JURISDICTION

Cyberspace poses unique legal challenges due to its borderless and decentralized nature, which often clashes with the territorial principles of traditional legal systems. Determining which country's courts have the authority to hear a cyber dispute or crime is one of the most complex issues in this domain.

1. Lack of Territorial Boundaries: Unlike physical crimes, cyber offenses can be committed from one country, affect systems in another, and involve data stored in a third. This makes it difficult to identify the appropriate legal forum.

2. Multiple Jurisdictions: One cyber incident like hacking, phishing or data theft can fall under the jurisdiction of multiple countries. This often leads to conflicts over which nation has the right to investigate or prosecute.

3. Conflict of Laws: Different countries have varying data protection, privacy and cybercrime laws. What may be legal in one jurisdiction could be crime in another, complicating international cooperation and enforcement.

4. Attribution Problems: Identifying the real perpetrator behind a cyber attack is challenging due to anonymity, VPNs and spoofing technologies. Without proper attribution establishing jurisdiction becomes nearly impossible.

5. Enforcement Limitations: Even when a country asserts jurisdiction, it may lack the practical ability to enforce its laws beyond its borders, especially if the accused is in a non-cooperative or hostile nation.

6. Absence of Universal Framework: There is no universally binding international treaty binding that governs cyber jurisdiction, leading to inconsistencies and gaps in

handling cross border cyber issues.[8]

CHAPTER VI: CONCLUSION & SUGGESTIONS

Cyberspace jurisdiction presents a complex legal challenge due to the global, borderless nature of digital activities. While countries like India have enacted statutes such as the IT Act, 2000 and updated codes like the Bharatiya Nyaya Sanhita, the legal framework still struggles to address cross-border cyber offences effectively. Issues like conflicting laws, difficulty in attribution, and limited enforcement capacity weaken the ability to ensure justice in cyberspace. A consistent, technology-aware legal approach is essential for securing digital environments while respecting international legal boundaries.

1. **Develop International Agreements**: Establish clear treaties or conventions to define jurisdiction in cybercrimes and enable smooth cooperation between nations.

2. **Harmonize Cyber Laws**: Encourage legal systems worldwide to adopt common definitions, penalties, and procedural rules for cyber offences.

3. **Set Up Cyber Dispute Tribunals**: Create specialized international or regional bodies to handle complex cross-border cyber disputes efficiently.

4. **Enhance Digital Evidence Standards**: Strengthen rules for collection, preservation, and admissibility of electronic evidence to support prosecution across borders.

5. **Invest in Cyber Forensics and Training**: Build technical capacity among law enforcement and judiciary to understand and tackle sophisticated cybercrimes.

6. **Encourage Public-Private Cooperation**: Partner with tech companies, ISPs, and cybersecurity firms to improve tracking, attribution, and response mechanisms.

[8] [Bhawna Kumari], *The Concepts and Issues of Jurisdiction in Cyberspace*, CorpBiz (July 25, 2023), https://corpbiz.io/learning/the-concepts-and-issues-of-jurisdiction-in-cyberspace/(last visited Jan 30, 2025).