Page 755 - 762 **DOI:** *https://doij.org/10.10000/IJLMH.112877*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 2

2022

A Sapient Approach to the Virtual Jurisdiction in India

AYUSHMAN TRIPATHI [1]

ABSTRACT

The invention of computers and computer networks has simplified life, and the internet has proven to be the icing on the cake. The use of the internet has transformed the world into a global village. Anyone, from wherever in the world, can now access internet resources in the blink of an eye. On the one hand, everything appears to be simple and straightforward, the other side of this online culture emphasizes the complexities and vulnerabilities associated with cybercrime.

The paper focuses primarily on the question of determining the jurisdiction of Indian courts in internet cases. The article provides an overview of certain statutes that use case law to address the country's jurisdictional issues. The goals of international conventions, as well as India's participation, have been addressed further. Furthermore, the essay offers a few solutions for overcoming the issue of cyber jurisdictional ambiguity.

I. INTRODUCTION

Today, a world without internet connectivity is unthinkable, since it has become a basic human requirement. Through its enormous contribution to communication and information sharing, this global network has made life easier for everyone. It has a significant impact on practically every aspect of life, including education, business, politics, medicine, infrastructure, and science and technology.

With the rise of internet culture came the concept of a virtual world known as Cyberspace, which is a virtual environment generated by interconnected computers and computer networks on the internet with no physical boundaries. Computers, networks, software, data storage devices, the Internet, websites, emails, and even electronic gadgets such as cell phones and ATM machines are all included in cyberspace.

Like every coin, cyberspace technologies have two sides, each with its own set of advantages and disadvantages. While there is no doubt that it has simplified our lives to a greater extent, the darker side of the story reveals that in recent years, computer technology and cyberspace

[1] Author is a student at Guru Ghasidas Vishwavidyalaya, Bilaspur, India.

 [ISSN 2581-5369]

have become an invitation to cyber threats.

The issue of cyber threat encompasses a wide range of criminal activities, from minor electronic crimes to more serious offenses such as illegal gambling, theft of personal information, cyberbullying, cyberstalking, cyber defamation, web jacking, data diddling, and so on. These offenses not only cause concern, but they also raise the question of jurisdiction in dealing with such cyber-crimes. Because cyberspace has no physical boundaries, criminals can easily access the system from anywhere in the world using a computer or other electronic device.

For example, someone sitting in China may sneak into an Indian bank's host computer and transfer millions of rupees to a Swiss bank in the blink of an eye. He would only need a computer and a cell phone to complete this task. Once a crime has been committed, there is a question of jurisdiction as to where the complaint should be filed for trial. This is due to the fact that different countries' regulations for dealing with cybercrime cases differ.

II. JURISDICTION WITH REGARD TO CYBERCRIME AND NATIONAL LAW

Jurisdiction is the authority or authority of the court to hear and decide on an issue and determine the issue that precedes it, or the authority of the court to recognize the issue raised before it, but with respect to the decision, it has jurisdiction. Comes in the context of cyberspace, which becomes a tiring part of the law.

In common parlance, Jurisdictions is of two types:

- The court's subject jurisdiction permits it to decide cases of a specific type and determine whether the claim is actionable in the court where the case was filed.
- Personal jurisdiction empowers a court to rule on issues involving citizens or residents of its territory who have a relationship to that territory, regardless of where they are now located. Every state has personal jurisdiction over the persons who live inside its borders.

The concept of jurisdiction can be better understood by referring to sections 15 to 20 of the Code of Civil Procedure (1908), which discuss the place of suing or subject matter jurisdiction, and section 20 of this code specifically refers to any other category of suit not covered by sections 15 to 19.

Section 20 serves important ingredients for the purpose of the institution of another suit

 [ISSN 2581-5369]

in a court within the local limits of whose jurisdiction[2]:

A. At the time the suit is filed, the defendant or each of the defendants resides operates a business, or works for a living.

B. Any of the defendants who resides, carries on business, or personally works for gain at the time of the commencement of the suit, provided that either the court grants leave, or the defendants who do not reside, carry on business or personally works for gain, as aforesaid, acquiesce in such institution, or the defendants who do not reside, or carry on business, or personally works for gain, as aforesaid, acquiesce in such

C. The cause of action wholly or partially arises.

This part, however, does not appear to be appropriate in the virtual world. The problem with cyberspace jurisdiction is that it involves multiple parties from all over the world who only communicate via virtual connections. As a result, we can't get a clear picture of the parties and the location of the lawsuit so that the court's jurisdiction to hear such cases can be determined.

The Information Technology Act, 2000 (IT Act), which went into effect on October 17, 2000, is the main source of cyber legislation in India. The Act's goal is to provide e-commerce legal legitimacy and make it easier for the government to store electronic information.

The IT Act also penalises and punishes numerous forms of cybercrime. There are several provisions in this legislation that render the idea of judicial jurisdiction for the trial of cases involving cyber crimes in India as well as beyond India.

Such provisions of the IT Act are as follows:

The first section of the legislation states the scope of its application. It goes like this[3]:

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any individual.

Section 75 of the Act deals with the laws that apply to offenses or violations committed outside of India. It stipulates that[4]

1. subject to the provision of subsection (2), the provision of this act shall also apply to any offense or contravention committed outside India by any person irrespective of his nationality.

2. For the purpose of subsection (1), this act shall apply to an offense or contravention

[2] Sec 20 of code of civil procedure 1908
[3] Information technology Act 2000
[4] ibid

 [ISSN 2581-5369]

committed outside India by any person if the act or conduct constituting the offense or contravention involves a computer, computer system or computer network located in India.

COMMENT: The IT Act's sections 1(2) and 75 apply to any offense or violation committed in India or abroad. Invoking the power of extraterritorial jurisdiction of the nation, this act can be used outside of India. It doesn't matter if the criminal is an Indian citizen or if the crime was committed inside or outside India. It applies to anyone who damages or attempts to damage a computer, computer system, or network, regardless of nationality. India by doing business from India or elsewhere in the world.

Sec 46 of the Act grants the Cyber Appellate Tribunal the power to adjudicate in the event of a violation of any provision of the Act, and it also allows for the appointment of an adjudicating officer who is vested with the powers of civil courts.

The establishment of a Cyber Appellate Tribunal is provided for under Section 48 of the act[5].

(1) The Central Government shall establish one or more appellate tribunals known as the Cyber Regulations Appellate Tribunal through notification.

COMMENT: The government establishes this tribunal under this Act, and the government selects what cases and where the tribunal will exercise its authority. It is regarded as the initial appellate tribunal to which appeals from the control board or adjudicating officer orders are preferred. Furthermore, anyone who is aggrieved by an appellate tribunal decision has sixty days from the date of communication of the decision or order to file an appeal in the High Court.

The Information Technology Act of 2000 appears to be comprehensive when it comes to adjudicating matters involving Indian citizens and offenses or contraventions committed in India, as Indian courts follow the principle of lex foris, or country law, but it still causes confusion when it comes to exercising its extraterritorial jurisdiction over offenses committed outside India or by those who are not a citizen.

For example, suppose an American citizen harmed the reputation of an Indian politician by posting filthy comments on social media, and the injured person sought justice in an Indian court. Although the IT Act of 2000 clearly provides for extraterritorial jurisdiction, the question remains as to how successful it would be to bring an American citizen to India to be punished for cyber defamation because the IT Act does not apply to Americans.

[5] Supra Note 2

 [ISSN 2581-5369]

Apart from the Information Technology Act of 2000, there is other relevant legislation under Indian law that allows Indian courts the ability to handle problems relating to cybercrime, such as:

The extraterritorial jurisdiction of Indian courts is also addressed in sections 3 and 4 of the Indian penal code of 1882[6].

Section 188 of the CrPC 1973 states that an offence committed by an Indian citizen outside the nation is subject to the jurisdiction of Indian courts. Section 178 deals with crimes done in India or parts of them, while Section 179 deals with the consequences of crimes committed in Indian territory[7].

III. RELEVANT CASE LAWS

SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra[8]

This is an example of defamation online. This is the first case of this kind in India, in which case the defendant is an employee of the plaintiff's company and is derogatory, obscene, vulgar, and abusive not only to his boss but also to various subsidiaries of companies around the world. I sent an e-mail. The purpose of sending these emails was to damage the reputation of companies and their CEOs around the world.

The Delhi High Court has taken jurisdiction over a case of corporate reputation defamation via e-mails. The court granted an ex-parte injunction.

SIL Import v. Exim Aides Silk Importers[9]

In this case, the court successfully underscored the need for judicial interpretation of the statute in light of recent technological advancements. Until there is specific legislation regarding the jurisdiction of Indian courts over Internet disputes, or unless India is a signatory to an International Treaty stipulating the jurisdiction of national courts and the circumstances in which they can be exercised, Indian courts will have to give the existing statutes a broad interpretation in order to exercise Internet disputes.

Impresario Entertainment & Hospitality Pvt. Ltd. vs S&D Hospitality[10]

The plaintiff's company, which has a registered office in Mumbai and operates in New Delhi, provides restaurant services and operates restaurants under the name and style of "SOCIAL"

[6] Sec 3 and 4 Indian penal code,1860
[7] Section 178, 179 and 188 of Code of Criminal Procedure, 1973.
[8] Suit No. 1279/2001 available at https://indiankanoon.org/doc/
[9] (1999) 4 SCC 567
[10] CS(COMM) 111/2017

 [ISSN 2581-5369]

with one brand and many locations. The plaintiff found out from a friend about the defendant's restaurant "SOCIAL MONKEY" in Hyderabad.

It also has a popular beverage called A GAME OF SLING, and the defendant has a beverage called Hyderabad Sling that is identical or deceptively similar to the plaintiffs. Both of these establishments have signed agreements with websites such as Zomato and Dine Out, and their information, including menus and contact information, was made public on their respective websites.

Therefore, the issue before the Delhi High Court was whether it had the jurisdiction to adjudicate the matter?

The Hon'ble Court also stated that in passing off or infringement action (where the plaintiff is not located within the court's jurisdiction), the plaintiff's business, goodwill, or reputation in the forum state must be damaged as a result of the Defendant's website being accessed in the forum state. As a result, the court determined that the website's mere interaction in the forum State did not entitle it to jurisdiction.

Previously, in Banyan Tree Holding (P) Limited v. A. Murali Reddy and Anr[11], the court concluded that a passive website with no aim of expressly targeting audiences beyond the State where the website's host is located cannot vest the forum court with jurisdiction.

IV. INDIA AND INTERNATIONAL CONVENTION OVER CYBER JURISDICTION

The Budapest Convention on Cybercrime, also known as the Convention on Cybercrime, was the first international convention to address the Internet and cybercrime by taking into account national laws, enhancing international cooperation, and strengthening investigative procedures. The Council of Europe, Canada, Japan, the Philippines, South Africa, and the United States all signed it at Strasbourg, France. Countries like India and Brazil, on the other hand, have refused to adopt the Treaty because they were not involved in its drafting. However, due to an increase in cybercrime, India has been revising its position on the convention since 2018.

Article 22 The Convention on Cyber Crime, 2001 allows the country to have jurisdiction if cybercrime is committed [12]:

- In its territory;
- Onboard a ship flying the flag of the country;

[11] CS (OS) No 894 of 2008
[12] ETS185 | Cybercrime (Convention) Budapest, 23.XI.2001

- Onboard an aircraft registered under the laws of the country
- By one of the country's nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

V. UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME (UNTOC)

In November 2000, the United Nations General Assembly passed a resolution approving this pact. India, as a participant, became an associate in 2002. The Palermo Convention, commonly known as the UNTOC, requires state parties to create domestic criminal offenses that target organized criminal groups, as well as new structures for extradition, mutual legal assistance, and law enforcement collaboration. Despite the fact that the treaty does not specifically include cyber-crime, its rules are extremely relevant[13]. The Information Technology Act of 2000 was enacted in India as a result of this accord.

VI. RECOMMENDATIONS

- In cases of cybercrime, there is a need for unique legislation that can be used to define jurisdiction. At the international level, a law must be drafted in collaboration with countries that are vulnerable to cyber threats.
- India has to become a more active participant in and signatory to agreements and treaties aimed at combating cybercrime and ensuring cyberspace security.
- To identify a court's jurisdiction, flaws in the legislation must be located, and relevant adjustments must be made to broaden the scope of adjudication.
- The legislation governing extradition policy must be drafted by the legislature.

VII. CONCLUSION

The rise in cybercrime has a negative impact on cyberspace, posing a threat to national security. Even if all required safeguards and cyber security measures are adopted, history demonstrates that it is nearly difficult to banish crime from the virtual world.

As a result, it's critical that strict regulations be enacted to deal with cybercrime, where the first and most crucial question is whether the court has the authority to hear the case.

Because cyberspace is a world with no boundaries, determining the power of a court to

[13] General Assembly resolution 55/25 of 15 November 2000

 [ISSN 2581-5369]

adjudicate on the topic is challenging. As a result, the need of the hour is to design a unique law that can be applied to cases of cybercrime without difficulty or confusion.

The latest cybercrime incident clearly demonstrates that India is also vulnerable to cyber dangers; therefore, in order to solve the issue, India should become a signatory to the Budapest Convention and ratify it. By demonstrating its global footprint, the country will be better able to combat cybercrime and resolve jurisdictional disputes.

*****

 [ISSN 2581-5369]