REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 13 | ISSUE - 9 | JUNE - 2024

JURISDICTIONAL CHALLENGES IN RESOLVING CYBER CRIME

Dr. Kalindri[1] and Ms. Ayushi Gupta[2]
[1] Assistant Professor of Law at Faculty of Law, University of Lucknow, Uttar Pradesh.
[2] Ph.D. Research Scholar at Faculty of Law, University of Lucknow.

ABSTRACT:

The ambit of Cyber law is so vast that cyber jurisdiction in a case involving various countries is very difficult to ascertain. A website, app, product, or content in one country may be legal but illegal in another, the parties may be residents or non-residents, which makes this concept all the more complex.Social media, online payments, online banking, online education, gaming, digital communication, and search engines have all become indispensable components of people's daily lives during the past 20 to 24 years, and they have also contributed to the rise in cybercrime through increased Internet misuse. The actual cause of this is a lack of strict legislation, knowledge, gaps in user safety and privacy, and other issues.

Criminal activity on the web (internet) is termed cybercrime.Since the accused and the victim in cybercrimes are typically from different nations, it can be difficult to determine whose cyber jurisdiction will rule in these cases.

There is no problem as long as a user's online behavior is lawful and does not break any regulations. But jurisdiction becomes important when these acts turn criminal and unlawful. A court's jurisdiction grants it the authority to hear a matter and render a decision.

KEYWORDS: *cyber crime, cyber space, jurisdiction, technology ,transaction, borders.*

I. INTRODUCTION

The ambit of Cyber law is so vast that cyber jurisdiction in a case involving various countries is very difficult to ascertain. A website, app, product, or content in one country may be legal but illegal in another, the parties may be residents or non-residents, which makes this concept all the more complex. Cyber law's jurisdiction depends on the kind of cybercrime and the location from which it has been done. The usage of computers, mobile phones, and other electronic devices has increased significantly over the 20th and 21st century transition periods. Subsequently, as internet usage increased, individuals started becoming dependent on it in the 1990s. Social media, online payments, online banking, online education, gaming, digital communication, and search engines have all become indispensable components of people's daily lives during the past 20 to 24 years, and they have also contributed to the rise in cybercrime through increased Internet misuse. The actual cause of this is a lack of strict legislation, knowledge, gaps in user safety and privacy, and other issues.

Criminal activity on the web (internet) is termed cybercrime. Cybercrime is prevented and protected by Cyber laws. The non-presence of physical boundaries on the internet and the non-effective security of the data of the user is one of the main reasons for cybercrime.

Because of the reason that internet has no boundaries and restraints, following challenges are being faced by the justice delivery mechanism:

1. No physical restraints lead to undefined jurisdictional boundaries of cybercrime.
2. Municipal boundaries of countries work according to laws applicable within their boundaries. The laws and definitions of different crimes are not necessarily be at par with that of other States.
3. Investigating agencies face difficulty in collecting information and data due to different structure of laws and applicability of laws in different jurisdictions.
4. The cybercrime modality works from lowest scale to highest of it which lead to unreported cases to shoot higher in number. Unclear jurisdictions of such number of crimes is indispensable.

II. WHAT IS CYBER JURISDICTION?

Cybercrime refers to illegal action that occurs through the internet. Cyber laws guard against and prevent cybercrime. One of the primary causes of cybercrime is the absence of physical borders on the internet and the inadequate security of user data.

A person may find themselves ensnared in cybercrime by a hacker, internet stalker, cyber-terrorist, fraudster, or many other individuals in another nation due to the rise in internet users and the availability of free global browsing content. Online fraud can occur, for example, when someone poses as a seller of a product from one nation to another, collects money online, and then fails to deliver the promised goods.

Cyberspace is also governed by cyberlaw. The term "cyberspace" describes the online communication-facilitating virtual environment on computers, and more precisely, an electronic medium. In cyberspace, a sizable computer network composed of numerous global computer sub-networks that use the TCP/IP protocol to facilitate data exchange and communication is the norm.[1] Conflicting laws arise from the internet's boundless nature, lack of restrictions, and the similarities between cybercrime and its characteristics. The methodologies taken by international law and municipal law differ, and cyber law is mostly a matter of overlap between the two, leaving no clear outcome.

III. ISSUES RELATED TO JURISDICTION IN CYBERSPACE

A court's jurisdiction grants it the authority to hear a matter and render a decision. Since the accused and the victim in cybercrimes are typically from different nations, it can be difficult to determine whose cyber jurisdiction will rule in these cases. As previously mentioned, the internet has no bounds, therefore no particular nation in cyberspace may claim ownership over its use. The user is allowed to access anything from anywhere at any time. There is no problem as long as a user's online behavior is lawful and does not break any regulations. But jurisdiction becomes important when these acts turn criminal and unlawful.

For instance, it is necessary to determine which country's jurisdiction will apply if a person uses the server of country "C" to execute a robbery in country "A" while seated in country "B." Even though the transaction in this instance may have been completed electronically, the parties involved are still physically present in the nations that govern them, and the court will usually determine which nation's cyber jurisdiction applies in this case.

A transaction in cyberspace often involves three parties: the user, the server host, and the party they are transacting with. All parties must fall under one cyberspace jurisdiction.[2] Since the three participants in this image are from three separate nations, it is unclear if the laws of "A," "B," or "C" will

[1] Techopedia (last visited June 04, 2024)

[2] Georgina Pereira, Cyber Space Jurisdiction: Issues and Challenges, Legal Bites , (last visited June 06, 2024)

apply in this situation. Additionally, it is unclear whether local laws or international laws will have jurisdiction over cyberspace. Another question is the extent to which a court can apply domestic state laws and hear a cross-border case.

IV. TYPES OF CYBERSPACE JURISDICTION

International law recognizes three types of cyber jurisdiction recognized, namely-

- **Personal Jurisdiction**: This sort of jurisdiction allows the court to make decisions about specific parties and individuals. The US Supreme Court noted in the ***Pennoyer v. Neff***[3] case that the US Constitution's due process clause limits personal jurisdiction by implication on non-residents; as a result, non-residents are not directly subject to jurisdiction. Nevertheless, the minimum contact hypothesis, which granted the authority over non-residents as well, limited this constraint.
- **Subject-matter jurisdiction**: This is a category of jurisdiction in which the court has the authority to hear and rule on certain cases involving a given subject matter. The plea will be refused and the plaintiff will have to file a case in the court that is relevant to the topic if the plaintiff sued in a different court but the exact subject matter is handled by another court. For example, since district consumer forums focus on consumer-related disputes, a complaint about a consumer good should be submitted there rather than in district court. In a same vein, NGT hears all environmental cases instead of district courts.
- **Pecuniary Jurisdiction:** This category of jurisdiction focuses mostly on financial issues. The suit's value shouldn't be greater than the financial jurisdiction. A court's jurisdiction to hear a matter is limited in numerous ways; cases that fall outside of these bounds are heard in other courts. The State consumer dispute redressal commission has financial jurisdiction over cases totaling more than 20 lakh rupees but not more than 1 crore, the National consumer dispute redressal commission has financial jurisdiction over cases totaling more than 1 crore rupees in India, and the district consumer forum, for instance, handles matters involving no more than 20 lakh rupees. It is hierarchically organized and based on the claims made during the proceedings.

V. PREREQUISITES OF CYBER JURISDICTION

There are three prerequisites of valid jurisdictions that are needed to be followed. A person is compelled to follow the rules and regulations of the state. The state has the power to punish a person violating such laws

- **Prescriptive Jurisdiction:** This kind of jurisdiction gives a nation the power to impose laws, specifically on an individual's behavior, status, situation, or preference. There is no limit to its jurisdiction. As a result, a nation may pass laws on any subject, even if the act took occurred in a different country or if the person's nationality differs. Nonetheless, no state may enact legislation that is in opposition to the interests of other nations under international law.
- **Jurisdiction to Adjudicate -** In civil or criminal cases, the state may exercise its jurisdiction over a party regardless of whether the state was a party; just a relationship between the parties is necessary for the state to make a decision. A state with prescribed jurisdiction does not necessarily need to have adjudicative jurisdiction.
- **Enforcement of jurisdiction** – Enforcing the jurisdiction is contingent upon the existence of prescriptive jurisdiction; in the event that prescriptive jurisdiction is lacking, this jurisdiction cannot be used to penalize an individual for breaking its laws and regulations. That being said, this jurisdiction is not absolute, and a state is not permitted to impose its jurisdiction on an individual or a crime that occurred in a foreign nation.

[3] Pennoyer v. Neff, 95 U.S. 714, 24 L. Ed. 565, 1877 U.S.

VI. THEORIES RELATED TO CYBERSPACE JURISDICTION

- **Subjective territoriality**: It stipulates that the parties shall be subject to the forum state's laws if the offense is committed there. The essential component under it is the non-resident person's act in the forum state. For instance, if a nation passes legislation making a certain behavior illegal within its borders, the relevant territoriality will acknowledge it.
- **Objective territoriality**: This principle is applied when an action is taken outside the borders of the forum state but nevertheless has an effect on the forum state. Another name for it is "Effect Jurisdiction." The principle was established in the ***United States v. Thomas***[4] case, where the plaintiff claimed it violated domestic laws. The defendant published phonographic material, and in order for subscribers to view and download it, he gave them a password after obtaining a form with their personal information on it. The court determined that "the effect of the defendant's criminal conduct reached the Western District of Tennessee, and that district was suitable for accurate fact-finding," indicating that the court has jurisdiction over cyberspace.
- The defendant in the historic case of ***Playboy Enterprise, Inc. v. Chuckleberry Publishing, Inc.***[5] ran an offensive photo-sharing website in Italy with some US citizens among its users. The court determined that the website violated US statutes and prohibited it from coming under US jurisdiction; nevertheless, the court lacks the authority to completely prohibit use of the website by users from other states because it does not have cyberspace jurisdiction.
- **Nationality:** This refers to the criminal who is a citizen of the state; for instance, if a citizen of a state commits a crime abroad that is punished under domestic law, the state may take legal action against the citizen.
- **Universality:** Crimes like child pornography and hijacking are widely acknowledged as crimes. Such a horrible act can result in a cybercriminal's conviction in any nation. In order to prosecute the perpetrator of a cybercrime, it is assumed that the nation has cyber jurisdiction.

EFFECTS TEST AND INTERNATIONAL TARGETING

A few requirements must be met in order to pass the Effect test, as mentioned in Objective Territoriality theory, chief among them being that the action must be taken specifically against the forum state with the knowledge and intent to harm the state. In internet disputes without contact, personal cyberspace jurisdiction is asserted if the court determines that the defendant's actions caused harm to the forum state.

The US Supreme Court noted that the state's court has personal jurisdiction over non-residents in the historic case of Calder v. Jones[6]. In this instance, an article defaming the inhabitants was published by the editor and writer of a major magazine. According to the case's circumstances, Shirley Jones filed a lawsuit against a national magazine's writer, distributor, and editor Calder for allegedly defaming her as an alcoholic. Although the piece was written and edited in Florida, Jones was a resident of California. Because the magazine was widely distributed throughout the state, Jones filed a lawsuit against the defendants in Californian court. The court decided that the defendants are under the personal jurisdiction of the Californian court.

In the case of ***Panavision International v. Toeppen***[7] Toeppen, the defendant engaged in cybercrime by profitably exploiting the plaintiff's brand and reselling it to him for a substantial sum. The California court determined that it had personal jurisdiction over the non-resident defendant by using the effects test.

[4] United States v Thomas ,74 F 3d 701(6th Cir 1996).
[5] Playboy Enterprise, Inc. v Chuckleberry Publishing; Inc., 939 F Supp 1032 (S.D.NY. 1996).
[6] Calder v Jones ,465 US 783 (1984).
[7] Panavision International v Toeppen,141 F 3d 1316 (9th Cir1998).

The Test evolved of Jurisdictional Aspects in Cyber Law

Cyberspace jurisdiction in cybercrime matters is determined by a number of tests. Which are as follows:-

- **Minimum Contacts Theory-**

When one or more parties are outside the court's territorial jurisdiction, this test is applied. In the historic decision in ***Washington v. International Shoe Company***[8], the US Supreme Court advanced this theory.[9] Following this instance, the court established three standards:

1. The claim must originate from or be the result of the defendant's forum-related activities, and
2. the exercise of jurisdiction must be reasonable.
3. "The non-resident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposely avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections."[10]

Thus, the court determined that contracts pertaining to cyberspace fall under the area of minimum contacts theory in the ***CompuServe Inc. v. Patterson***[11] decision.

- **Sliding Scale Theory**

Another name for sliding scale theory is the Zippo Test. It is the most often used test for determining personal jurisdiction in instances involving the internet. The websites' interactive features are used to determine jurisdiction. The forum state's courts have personal jurisdiction over an increased number of interactions. The courts may or may not have jurisdiction over a middle-range website, but they have cyberspace jurisdiction over a highly interactive website. In contrast, the courts have virtually little authority over inactive websites.

In another instance, Zippo Manufacturer, a Pennsylvania-based manufacturer of lighters, filed a landmark lawsuit against Zippo.com[12] alleging trademark infringement. It was determined that due to the defendant's high level of interaction, personal jurisdiction over them will apply.

VII. JURISDICTION UNDER INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 stipulates in section 1(2) that the Act covers the entirety of India and also applies to any offense or violation thereunder committed by any person outside India.[13]

Furthermore, Section 75 declares that "any offence or contravention committed outside India by any person, irrespective of his nationality, shall also be subject to the provision of sub-section (2)." For the purposes of sub-clause (1), any act or conduct that includes a computer, computer system, or computer network located in India qualifies as an offense or violation that is performed outside of India by any person.[14] This establishes prescriptive jurisdiction over Internet in India, and both residents and non-residents will face consequences for any actions they take that violate this Act.

---

[8] 326 US 310 (1945), 317 See Burk, Dan L. "Jurisdiction in a World Without Borders" 1 Va. J.L. & Tech. 3 (Spring, 1997) www.vjolt.net/vol1/issue/vol1_art3.html (accessed on 18th June, 2024.).

[9] Tricia Leigh Gray, "Minimum Contacts in Cyberspace: The Classic Jurisdiction Analysis in a New Setting", 2002 Journal of High Technology Law, http://www.jhtl.org/docs/pdf/ TGRAYV1N1N.pdf, (accessed on 19th June, 2024).

[10] Karnika Seth: Computer Technology Law, Chapter 2 Jurisdiction in the Borderless Cyberspace, (last visited June 05, 2024), http://www.karnikaseth.com/wp-content/uploads/Karnika%20Seth's%20Computers%20Inernet%20%20New%20Technology%20Laws.pdf

[11] CompuServe Inc v Patterson, 89F 3d 1257(6th Cir1996).

[12] Zippo Manufacturer v Zippo.Com, 952 F Supp 1119 (DCWD Pa 1997).

[13] Information Technology Act, 2000, section 1(2).

[14] *Id* at 13.

VIII. CONCLUSION

Even though different standards for determining cyberspace jurisdiction have been established, determining the jurisdiction in cybercrime cases involving many nations remains a contentious issue in legal forums. Different governments use different criteria to define jurisdiction. It is therefore very difficult to assert the jurisdiction of one nation over another when the disputed parties are from different states. A test of jurisdiction may therefore be valid in one country but invalid in another. In this case, determining the jurisdiction should take into account multiple tests.

But as the world's population will use the Internet more and more every second, rules pertaining to their jurisdiction should also be innovative enough to tackle cybercrime. Certain guidelines for determining jurisdiction should be established by international law, and cases where jurisdiction cannot be determined should be tried in the International Court of Justice.