

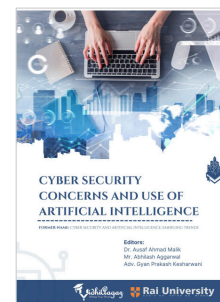
CHAPTER 47

Addressing Jurisdictional Challenges in Combatting Cyber Crimes: Pathways for the Future

Atul Jaybhaye

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 390–399

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Atul Jaybhaye, *Addressing Jurisdictional Challenges in Combatting Cyber Crimes: Pathways for the Future*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 390 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Atul Jaybhaye, 'Addressing Jurisdictional Challenges in Combatting Cyber Crimes: Pathways for the Future' in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 390.

CHICAGO (17TH ED.)

Jaybhaye, Atul. "Addressing Jurisdictional Challenges in Combatting Cyber Crimes: Pathways for the Future." In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 390–399. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-47/>.

APA (7TH ED.)

Jaybhaye, A. (2024). Addressing jurisdictional challenges in combatting cyber crimes: Pathways for the future. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 390–399). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-47/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-47/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

ADDRESSING JURISDICTIONAL CHALLENGES IN COMBATTING CYBER CRIMES: PATHWAYS FOR THE FUTURE

Dr. Atul Jaybhaye¹¹²

ABSTRACT

With the rapid advancement of digitization and technology, the usage of e-commerce, social media platforms, online banking, and digital communication services has surged among Internet users. Consequently, the last few years have witnessed a significant rise in cybercrime. In 2022, India recorded a 24% increase in cybercrime cases compared to 2021, according to the “National Crime Records Bureau (NCRB).” This rise occurred alongside increases in other types of crime, such as economic offences (11%), crimes against senior citizens (9%), and crimes against women (4%). While “the Information Technology Act, 2000” (IT Act, 2000) does not specifically define the term ‘cybercrime,’ it is generally understood as any crime in which a computer serves as either a tool or a target. Cybercriminals are constantly evolving their tactics, employing increasingly sophisticated methods to perpetrate fraud and other illegal activities. Although law enforcement agencies are working diligently to investigate these crimes, they face numerous challenges—foremost among them is determining jurisdiction in cybercrime cases. Jurisdictional criteria vary widely between countries, and the IT Act, 2000, provides limited guidance on the matter, addressing jurisdiction primarily through Section 75. Moreover, recent legislative measures such as the “Bharatiya Nyaya Sanhita, 2023,” (BNS) and the “Bharatiya Nagarik Suraksha Sanhita, 2023”, (BNSS) offer little in the way of resolving jurisdictional issues in cyberspace. Consequently, the Indian judiciary often relies on legal tests and theories developed in U.S. jurisprudence, such as the “Minimum Contacts Theory,” “Sliding Scale Theory,” and the “Effects Test”, to determine jurisdiction in cybercrime cases. This paper critically analyzes the jurisdictional challenges faced in the investigation of cybercrimes and offers recommendations to effectively address these issues, thereby enhancing the ability of law enforcement and judicial systems to combat cybercrime in the future.

Keywords: Cybercrime, Jurisdiction, IT Act, 2000, Digital investigation, Minimum Contacts Theory

INTRODUCTION

The age of information technology has profoundly transformed human life. The internet has become an essential part of daily existence, spanning all age groups from children to the elderly. Notably, even the Hon'ble Supreme Court of India has acknowledged the significance of internet access, affirming it as a fundamental right that cannot be unjustly denied.¹¹³ With the rapid progress of digitization, the use of e-commerce, social media platforms, online banking, and digital communication services has surged among Internet users. However, technology acts as a double-edged sword, bringing both benefits and drawbacks. While many individuals harness technology for lawful and productive purposes, cybercriminals exploit it to commit various offenses, including phishing, child pornography, cyber terrorism, and the creation of deepfake videos. Consequently, the past few years have seen a significant rise in cybercrime. In 2022, India recorded a 24% increase in cybercrime cases compared to 2021, as per the (NCRB). This spike coincided with increases in other crimes, such as economic offenses (11%),

¹¹² Assistant Professor (Law), Hidayatullah National Law University, Raipur, Chhattisgarh.

¹¹³ Available at “<https://www.indiatoday.in/news-analysis/story/internet-access-fundamental-right-supreme-court-makes-official-article-19-explained-1635662-2020-01-10>” (last visited on September 9, 2024).

crimes against senior citizens (9%), and crimes against women (4%).¹¹⁴ Despite the diligent efforts of law enforcement agencies to combat cybercrime, they face considerable challenges, particularly in determining jurisdiction. Jurisdictional criteria vary between countries, and when a cybercrime is committed by a foreign national targeting a computer system in India, jurisdictional complexities often arise. Law enforcement agencies and courts frequently struggle to ascertain the appropriate jurisdiction and the applicable laws, rules, and regulations, as these crimes occur in the virtual realm of cyberspace.

CONCEPT OF JURISDICTION

Jurisdiction is derived from two Latin terms: “*juris* (meaning law) and *diction* (meaning to speak).” Essentially, jurisdiction answers the question of which forum is appropriate and has the authority to “speak the law.” According to “Black’s Law Dictionary”, jurisdiction refers to “a court’s power to resolve a case or issue a decree.” The concept of jurisdiction exists to ensure that courts only handle matters that are within their legitimate scope, whether based on territorial boundaries or financial thresholds. Jurisdiction is rooted in public international law, conflict of laws, constitutional law, and the powers of the government’s executive and legislative branches to allocate resources in a way that best serves societal needs.¹¹⁵

JURISDICTION IN CYBERSPACE

In cyberspace, jurisdiction poses a significant challenge for both domestic and international courts. If cyberspace is not treated as a global domain, it complicates traditional conflict-of-law principles, rendering them ineffective. Unlike conventional jurisdictional disputes, which may involve a few conflicting legal systems, even a basic webpage can be subject to the laws of multiple jurisdictions. To address this, cyberspace jurisdiction demands well-defined principles based on international law. Only by adopting such principles can courts worldwide work toward uniform solutions for resolving Internet jurisdiction issues.¹¹⁶

“The scope of cyber law is so extensive that defining jurisdiction in cases involving multiple countries can be very challenging. What may be legal in one country—whether it is a website, app, product, or content—could be illegal in another. Additionally, the parties involved could be residents or non-residents, further complicating the issue. Cyber jurisdiction is typically determined by the nature of the cybercrime and the location from which it was committed. Jurisdiction grants authority to the relevant court to hear a case and deliver a verdict. In cybercrime cases, the victim and the accused are often located in different countries, leading to conflicts over which jurisdiction should apply. While users are generally free to access content from anywhere, jurisdiction becomes critical when their online activities cross into illegal or criminal territory.”¹¹⁷

¹¹⁴ Available at “<https://indianexpress.com/article/india/rise-cybercrime-2022-economic-offences-ncrb-report-9053882/>” (last visited on September 9, 2024).

¹¹⁵ Mr. Amit Karkhanis, “An Overview of The Concept of Jurisdiction”, available at <https://www.livelaw.in/law-firms/article/s/concept-of-jurisdiction-173713> (last visited on September 11, 2024).

¹¹⁶ Darrel C. Menthe, “Jurisdiction in Cyberspace: A Theory of International Spaces,” 4 *Michigan Telecommunications and Technology Law Review*, 70 (1998).

¹¹⁷ Available at “<https://lawbhoomi.com/jurisdictional-aspects-in-cyber-law-and-information-technology-act/>” (last visited on September 13, 2024).

Traditionally, jurisdiction is determined by where the cause of action arises, but in cases involving multiple parties from different parts of the world, this becomes complicated. In cyberspace transactions, there are typically three key parties: the user, the service provider, and the person or business involved in the transaction. Ideally, the most appropriate legal framework should determine whether an event in cyberspace is governed by the laws of the state or country where the user is located, or if the laws of all other relevant countries or states should also apply. Unlike conventional transactions, cyber interactions involve the user, the server host, and the party with whom the transaction occurs, raising the fundamental question: which country's law should prevail?

Key issues arise when determining:

- In cross-border interactions, on what basis do we determine which country's law applies and which court has jurisdiction?
- What criteria allow a nation to apply its laws and regulations when the internet activity originates from a different jurisdiction?

In such cases, matters of jurisdiction fall under both state and international law, particularly when the parties involved are from different nations. Under international law, a state can apply its legal framework when international parties are involved in a dispute.¹¹⁸

TYPES OF JURISDICTIONS

International law identifies three types of jurisdictions in cyberspace:

Personal Jurisdiction – This type of jurisdiction permits a court to issue judgments specifically over certain individuals or parties. In *Pennoyer v. Neff*, the U.S. Supreme Court ruled that the Due Process Clause of the U.S. Constitution limits the exercise of personal jurisdiction over non-residents, meaning courts generally cannot assert direct jurisdiction over individuals who do not reside within the state. However, this limitation was later modified by the "minimum contacts" theory, which permits courts to exercise jurisdiction over non-residents if they have enough connections or interactions with the state.

Subject-matter jurisdiction – This type of jurisdiction allows a court to decide cases related to specific subject matters. If a case is filed in a court that does not have jurisdiction over the particular subject matter, the case will be dismissed, and the plaintiff must be refiled in the appropriate court. For example, a complaint concerning a consumer product must be filed in a district consumer forum, which specializes in consumer-related cases, rather than in a district court. Similarly, environmental disputes are handled by the National Green Tribunal (NGT), not by district courts, as the NGT has exclusive jurisdiction over environmental matters.

Pecuniary Jurisdiction – This type of jurisdiction pertains to financial matters, specifically where the value of a suit must fall within the court's pecuniary limits. Courts have defined monetary thresholds, and cases exceeding these limits must be tried in higher courts. For example, the district consumer forum handles disputes involving amounts up to ₹20 lakh, the State Consumer Dispute Redressal

¹¹⁸ Ms. Prevy Parekh & Ms. Tarunya Rao, "Cyberspace and Jurisdiction", 2 *Journal on Contemporary Issues of Law* 5 (2016).

Commission handles cases exceeding ₹20 lakh but below ₹1 crore, and the National Consumer Dispute Redressal Commission addresses cases involving amounts over ₹1 crore in India. This system is structured hierarchically based on the claim's value in the proceedings.¹¹⁹

Legal framework of Jurisdiction in India:

Extraterritorial jurisdiction – Cybercrimes: (Bharatiya Nyaya Sanhita, 2023)

“The provision of this Sanhita 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; and
- (c) any person in any place without and beyond India committing offence targeting a computer resource located in India.¹²⁰

Explanation - In this section, the word “offence” includes every act committed outside India which, if committed in India, would be punishable under this Sanhita.”

“The Information Technology Act, 2000”

“Sec. 75 – Act to apply for offence or contravention committed outside India.” -

- (1) “Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.
- (2) For the purposes of sub-section (1), this Act shall apply to an 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.”¹²¹

Sec. 75 of the IT Act, 2000 has a broader scope compared to Sec. 1(5) of the BNS, 2023. Section 75 applies to offences committed abroad involving a computer, computer system, or computer network located in India, while the BNS limits jurisdiction to cases where the targeted computer resource is within India. However, Sec. 75 has its limitations. For instance, if an offence under the IT Act is committed by a foreign national outside India and affects a computer system in India, but the act is not considered an offence in that foreign country, an Indian court's judgment may not be enforceable in that foreign jurisdiction. This is because the foreign court may not recognize the extraterritorial jurisdiction outlined in Sec. 75 if the act is legal in that country.¹²²

Sec. “199 -Offence triable where act is done or consequence ensues.” (“Bharatiya Nagarik Suraksha Sanhita, 2023”)

“When an act is an offence by reason of anything which has been done and of a consequence which has ensued, the offence may be inquired into or tried by a Court within whose local jurisdiction such thing

¹¹⁹ *Supra* note 5.

¹²⁰ Bharatiya Nyaya Sanhita, 2023, s. 1(5).

¹²¹ The Information Technology Act, 2000, s. 75.

¹²² Nishant Verma, Jurisdiction in Cybercrimes and Civil Disputes, available at

“<https://www.scconline.com/blog/post/2024/03/24/jurisdiction-in-cybercrimes-and-civil-disputes/>”(last visited on September 17, 2024).

has been done or such consequence has ensued.”

Sec. 202 – “Offences committed by means of electronic communications, letters,” etc. (BNSS 2023)

“(1) Any offence which includes cheating, may, if the deception is practised by means of electronic communications or letters or telecommunication messages, be inquired into or tried by any Court within whose local jurisdiction such electronic communications or letters or messages were sent or were received; and any offence of cheating and dishonestly inducing delivery of property may be inquired into or tried by a Court within whose local jurisdiction the property was delivered by the person deceived or was received by the accused person.

(2) Any offence punishable under section 82 of the Bharatiya Nyaya Sanhita, 2023 may be inquired into or tried by a Court within whose local jurisdiction the offence was committed or the offender last resided with his or her spouse by the first marriage, or the wife by the first marriage has taken up permanent residence after the commission of the offence.”

THE EVOLUTION OF JURISDICTIONAL TESTS IN U.S. JUDICIAL PRACTICE

1. Minimum Contacts Theory

This test is applicable when either or both parties are located outside the court's territorial jurisdiction. In the landmark judgment in “*Washington v International Shoe Company*”,¹²³ this theory was originated by the US Supreme Court.¹²⁴

After this case, the court has come up with three criteria-

- “The non-resident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections.
- the claim must be one that arises out of or results from the defendant’s forum-related activities, and
- exercise of jurisdiction must be reasonable.”

In the case of “*CompuServe Inc v Patterson*”¹²⁵, The court ruled that contracts involving cyberspace are also subject to the minimum contacts theory.

2. Sliding Scale Theory

“The Sliding Scale theory, commonly referred to as the Zippo Test, is a widely accepted framework for determining personal jurisdiction in cyberspace cases. This test assesses the level of interactivity of websites to establish jurisdiction. Generally, the more interactive a website is, the greater the likelihood that courts will assert personal jurisdiction over it in the forum state. For passive websites, courts

¹²³ 326 US 310 (1945).

¹²⁴ Karnika Seth, “Jurisdiction in the Borderless Cyberspace”, available at “<http://www.karnikaseth.com/wp-content/uploads/Karnika%20Seth’s%20Computers%20Inernet%20%20New%20Technology%20Laws.pdf>” (last visited on September 17, 2024).

¹²⁵ 89F 3d 1257(6th Cir1996).

typically have little to no jurisdiction. In cases of websites that fall somewhere in the middle, jurisdiction may be uncertain, while highly interactive sites usually grant courts clear jurisdiction in cyberspace.”¹²⁶

In the landmark case of “*Zipco Manufacturer v Zipco.Com*”¹²⁷, the plaintiff Zipco Manufacturer of lighters in Pennsylvania filed a suit against the defendant Zipco.com for trademark violation. The defendant had sufficient interactivity; therefore, the personal jurisdiction was made applicable to the defendant.

3. Effects Test and International Targeting

To satisfy the Effect test, certain conditions must be fulfilled: primarily, the action should be directed precisely at the forum state with the knowledge and intent to cause harm there. If the court decides that the defendant's actions have indeed caused injury to the forum state, it can assert personal jurisdiction in cyberspace cases even when there are no direct contacts. This approach allows courts to extend their jurisdiction based on the foreseeable effects of a defendant's conduct on the forum state, emphasizing the impact of the action rather than the location of the parties involved.

In the famous case of “*Calder v Jones*”¹²⁸, the U.S. Supreme Court held that a court can exercise personal jurisdiction over non-residents in certain cases. In the case of *Shirley Jones*, she filed the suit against the distributor, writer, and editor of a national magazine for defamation after they labeled her an alcoholic. Albeit, the article was written and edited in Florida, Jones filed her lawsuit in California due to the magazine's substantial distribution there. The court ruled that California had personal jurisdiction over the defendants, highlighting the article's impact within the state.

In “*Panavision International v Toeppen*”,¹²⁹

The defendant was engaged in cybercrime by using the plaintiff's trademark commercially and attempting to sell it back to him at a high price. The California court applied the effects test and ruled that it had personal jurisdiction over the non-resident defendant due to the intentional harm caused to the plaintiff in California.

OTHER COMMON LAW JURISDICTIONS

Next, we will examine the approach taken by courts in other common law jurisdictions, including India.¹³⁰

Canada

In “*Morguard Investments Ltd. v. De Savoye*,”¹³¹ the Canadian Supreme Court established the "real and substantial connection" test for ascertaining jurisdiction. The court noted that allowing a suit to proceed based on this connection strikes a fair and reasonable balance between the rights of the parties involved. In “*Pro-C Ltd. v. Computer City Inc.*”¹³² the court ruled that the defendant's listing of

¹²⁶ *Supra* note 5.

¹²⁷ 952 F Supp 1119 (DCWD Pa 1997).

¹²⁸ 465 US 783 (1984).

¹²⁹ 141 F 3d 1316 (9th Cir1998).

¹³⁰ Justice S. Muralidhar, “Jurisdictional Issues in Cyberspace,” *Indian Journal of Law and Technology*, 6, 22-26, (2010).

¹³¹ [1990] 3 S.C.R. 1077 (Can.).

¹³² 7 C.P.R. (4th) 193 (Can.), rev'd, 205 D.L.R. (4th) 568 (Can.).

Canadian retail outlets on their website, combined with the existence of a de facto "common market" between Canada and the U.S., indicated that Canadian consumers were targeted. As a result, the Ontario court had jurisdiction to hear the trademark violation case against the defendant based in the U.S.

In “*Patrick Desjean v. Intermix Media Inc.*”¹³³ “The defendant, a Delaware corporation with its principal office in Los Angeles, offered seemingly free software programs. When the plaintiff, a Canadian resident, installed a free screensaver or game from www.mycoolscreen.com, he unintentionally also installed spyware. Subsequently, the plaintiff filed a lawsuit against the defendant in Canada for violating the misleading representations provisions of the Canadian Competition Act, 1985.” The Federal Court of Ottawa, after stating to the decision of the Ontario Court of Appeal in “*Muscutt v. Courcelles*,” (2002) 213 D.L.R. (4th) 577, considered the following eight factors to determine whether it had jurisdiction:

- (1) “The connection between the forum and the plaintiff’s claim; (2) The connection between the forum and the defendant; (3) Unfairness to the defendant in assuming jurisdiction; (4) Unfairness to the plaintiff in not assuming jurisdiction; (5) Involvement of other parties to the suit; (6) The Court’s willingness to recognize and enforce an extra-provincial judgment rendered on the same jurisdictional basis; (7) Whether the case is interprovincial or international in nature; (8) Comity and standards of jurisdiction, recognition and enforcement prevailing elsewhere.”

The court noted that the defendant had no office in Canada, although it previously subsidized office space for contractors on two websites acquired by Intermix. Additionally, there were no servers in Canada for www.mycoolscreen.com; it was hosted on a server in California. The data revealed that 66% of downloads came from American users, while Canada accounted for only 2.5% to 5.3% of downloads. Given these factors, the Federal Court ruled that Canadian courts lacked jurisdiction over the defendant due to the absence of a substantial connection with the forum. Notably, the court recognized the importance of reciprocity in enforcing extra-provincial judgments, emphasizing that without it, exercising personal jurisdiction over extraterritorial defendants could be ineffective.¹³⁴

United Kingdom

In “*1-800 Flowers Inc. v. Phonenames*”¹³⁵

The defendant was a UK-based phonebook company, while the plaintiff operated a flower delivery business accessible globally through its website. However, there was no evidence that UK residents had actually placed orders on the site. The argument was made that since the website was accessible from the UK, the defendant's use of the mark "1-800" constituted use in the UK. In the first appeal, the bench ruled that the mere accessibility of websites worldwide did not equate to trademark use in all those jurisdictions. The court emphasized that the website owner's intention and how users would interpret

¹³³ 2006 F.C. 1395 (Can.).

¹³⁴ *Supra* note 18.

¹³⁵ [2002] F.S.R. 12 (C.A.) (U.K.).

the website were relevant factors. The Court of Appeals also dismissed the argument, with Justice Buxton noting that...

“I would wish to approach these arguments, and particularly the last of them, with caution. There is something inherently unrealistic in saying that A ‘uses’ his mark in the United Kingdom when all that he does is to place the mark on the internet, from a location outside the United Kingdom, and simply wait in the hope that someone from the United Kingdom will download it and thereby create use on the part of A. By contrast, I can see that it might be more easily arguable that if A places on the internet a mark that is confusingly similar to a mark protected in another jurisdiction, he may do so at his peril that someone from that other jurisdiction may download it; though that approach conjured up in argument before us the potentially disturbing prospect that a shop in Arizona or Brazil that happens to bear the same name as a trademarked store in England or Australia will have to act with caution in answering telephone calls from those latter jurisdictions. However that may be, the very idea of ‘use’ within a certain area would seem to require some active step in that area on the part of the user that goes beyond providing facilities that enable others to bring the mark into the area. Of course, if persons in the United Kingdom seek the mark on the internet in response to direct encouragement or advertisement by the owner of the mark, the position may be different; but in such a case the advertisement or encouragement in itself is likely to suffice to establish the necessary use.”¹³⁶

India:

“Casio India Co. Limited v. Ashita Tele Systems Pvt. Ltd”.¹³⁷ “in this passing off action, the defendant operated a business in Bombay and had registered the domain name www.casioindia.com, with the second defendant serving as the Registrar for this domain. The plaintiff claimed to be a 100% subsidiary of Casio Computer Ltd. in Japan (Casio Japan), which owned the registered trademark “Casio” in India, and associated with various electronic products. The plaintiff had also registered multiple domain names in India, including “CasioIndiaCompany.com,” “CasioIndia.org,” and “CasioIndia.net.” The first defendant obtained the contested domain name during a period when it held a distributorship agreement with the plaintiff.” It was observed by the learned single Judge after referring to the decisions in **Rediff Communication Ltd. v. Cyber Booth**¹³⁸ and **“Dow Jones & Co. Inc. v. Gutnick”**¹³⁹ that “once access to the impugned domain name website could be had from anywhere else, the jurisdiction in such matters cannot be confined to the territorial limits of the residence of the defendant.”¹⁴⁰ According to the learned single Judge, since a mere likelihood of deception, whereby an average person is likely to be deceived or confused was sufficient to entertain an action for passing off, it was not at all required to be proved that “any actual deception took place at Delhi. Accordingly, the fact that the website of Defendant No. 1 can be accessed from Delhi is sufficient to invoke the territorial jurisdiction of this Court.”¹⁴¹

¹³⁶ *Ibid.*

¹³⁷ 2003 (27) P.T.C. 265 (Del.) (India), overruled by *Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy*, CS(OS) 894/2008 (High Court of Delhi, 23rd November 2009) (India).

¹³⁸ A.I.R. 2000 Bom. 27 (India).

¹³⁹ (2002) H.C.A. 56 (Austl.).

¹⁴⁰ *Supra* note 25.

¹⁴¹ *Ibid.*

In “*India TV Independent News Service Pvt. Limited v. India Broadcast Live Llc & Ors.*”,¹⁴² a different approach was adopted. India TV sued India Broadcast Live LLC for cybersquatting, alleging the defendants registered the domain name "indiatvlive.com," which was deceptively similar to the plaintiff's well-known trademark "India TV." The court held that domain names are subject to trademark law principles and ruled in favor of India TV, recognizing that the unauthorized use of the domain name amounted to passing off and infringement of intellectual property rights. The court granted a permanent injunction. It was also held that the mere fact that a website is available in a specific location might not be enough for the courts of that location to exercise personal jurisdiction over the website's owners. The situation would be different if the website was not only passive but also interactive, allowing browsers to not only access the contents but also subscribe to the services provided by the owners.

Both Casio and India TV were decisions of single Judges and required proper reconciliation. The opportunity presented itself in “*Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy*”¹⁴³ the plaintiff was a company located in Singapore. It claimed that it was part of a group of companies involved in the hospitality business. It claimed the use of the word mark ‘Banyan Tree’ and the banyan tree device since 1994. The plaintiff maintained the websites ‘www.banyantree.com’ and ‘www.banyantreespa.com’ since 1996. The websites were accessible in India. Its application for the registration of the mark and the device was also pending. In October 2007, the plaintiff learnt that the defendants, located in Hyderabad in Andhra Pradesh, had initiated work on a project under the name ‘Banyan Tree Retreat’, which according to the plaintiff was deceptively similar to that of the plaintiff. The plaintiff invoked the jurisdiction of the Delhi High Court, arguing that the defendants' website, www.makprojects.com/banyantree, which advertised their products and services, was accessible in Delhi. The plaintiff claimed that the use of a deceptively identical mark would mislead the public, thereby seeking an injunction. The Division Bench of the Delhi High Court, while addressing a referral from a Single Judge, affirmed its ruling in India TV and overruled Casio. The key issue was whether the Delhi court had jurisdiction, given that the defendant was based outside Delhi. The court established the "purposeful availment" test for online jurisdiction, stating that courts could assert jurisdiction if the defendant intentionally targeted customers in the plaintiff's jurisdiction, leading to harm there. Ultimately, the court dismissed the suit due to a lack of sufficient evidence showing targeting.

CONCLUSION

Addressing jurisdictional challenges in combatting cybercrimes under the IT Act, 2000 requires an understanding of how cyberspace defies traditional territorial boundaries. The Act provides a framework, but challenges remain due to the global nature of the internet. Jurisdiction is typically determined through three tests: the Territorial Nexus Test, where jurisdiction is based on a connection to the territory; the Effects Test, which grants jurisdiction if the crime significantly impacts a specific country; and the Targeting Test, where jurisdiction is determined if a cyber activity intentionally targets a particular region. However, these tests face limitations in a digital world, where hackers often operate across multiple jurisdictions, masking their locations and impacts. To overcome these obstacles, several

¹⁴² 2007 (35) P.T.C. 177 (Del.) (India).

¹⁴³ CS(OS) 894/2008.

steps must be taken. First, the IT Act should be regularly updated to reflect new technological realities, including clearer guidelines for cross-border cybercrimes. International cooperation is essential, particularly through stronger agreements like Mutual Legal Assistance Treaties (MLATs) and adopting global frameworks such as the Budapest Convention. Furthermore, law enforcement must be equipped with advanced training and resources to tackle complex cybercrime investigations, particularly those involving cross-border issues. Collaboration with private tech companies is critical, as they hold vital data that can assist in tracking cybercriminals. Establishing effective public-private partnerships will help bridge the gap between law enforcement and the tech sector, expediting the investigative process. By focusing on updating legal frameworks, fostering international cooperation, and enhancing cybersecurity capabilities, the jurisdictional challenges in cybercrime investigations can be mitigated, ensuring a more secure and responsive approach to digital threats.
