

JURISDICTION ISSUES IN CYBER CRIMES: A CHALLENGING APPROACH

Dr. Hemlata Sharma

Associate Professor, IIMT & School of Law (GGSIPU) Delhi

Kiran Mishra

BA, LLB. V Year Student, IIMT & School of Law (GGSIPU) Delhi

ABSTRACT

The cyber space is a realm and this virtual realm is almost as big as the physical realm. The cyber space is the whole of the internet and the intranet. The accessibility of this space doesn't question its existence. The cyber space witnesses multi-natured transactions each moment. These transactions may or may not be required to be secured depending on the parties to the transaction. Where the transactions are not secured and are vulnerable to cyber-attacks, the parties may suffer loss. The loss might not always be restricted to a monetary kind, but it may be physical, emotional and even a loss to the reputation or all of it at the same time. Thus, there arises a need to deal with cybercrimes and the need of surveillance in the cyber-space.

With the advent of cyber laws arose the need of defining jurisdiction of various courts of justice. The cyber space does not have a physical existence; thus, the exercise of jurisdiction becomes even more inconvenient. The offences in the cyber space are not as conveniently and practically traced as the offences which are committed in the physical realm. Offences in the cyber-space may be committed from virtually any place in the world, but the real location of the offender may or may not be in the jurisdiction of the trying court and a court without a definite jurisdiction cannot do justice. The victim may be under the jurisdiction of the trying court, but the court, may be, still hindered in trying the offenders or even investigating the offence due to non-conforming international laws. Hence, this paper attempts to all the issues of jurisdiction incidental to cybercrimes.

Keywords : *Cyber, cybercrimes, cyberattacks*

1. INTRODUCTION

Cyberspace has no territorially based boundaries, because the cost and speed of transmission of any message on the Net is almost entirely independent of physical location. Messages can be transmitted from one physical location to any other location without degradation, decay, or substantial delay, and without any physical cues of barriers that might otherwise keep certain geographically remote places and people separate from one another. The Net enables transactions between people who do not know and in many cases cannot know each other's physical location. The power to control activity in cyberspace has only the most tenuous connections to physical location.(Verma, Mittal, 2017)

As the users and system operators encounter conflicts and seek to resolve disputes, they act to establish rules and decide individual cases. The internet's decentralized nature makes it likely that any given internet transaction will involve parties from more than one jurisdiction.

All this creates a new form of law, a law of cyberspace, based on private contracting on a global basis and enforced by a combination of the system operator ultimate right to banish unruly users and the user ultimate right to migrate to other online service providers. Cyberspace requires its own set of jurisdictional rules, thus extinguishing geographical borders. Certain aspects of the internet have been compared to surface mail and telephone systems as well as advertisements in the national publications. (Singh, 2016).

Jurisdiction is the authority granted to the court to deal with and make resolutions on legal disputes. Traditional law is based on the notion that activity occurred in a particular jurisdiction as a nation, a state or territory or a municipality and can be dealt through reference and the rules and authorities of that physical location.

2. NATIONAL PERSPECTIVE OF JURISDICTION ISSUE IN CYBERSPACE

These are the following categorization regarding the National jurisdiction issues-

2.1 Personal Jurisdiction- An authority over a person, regardless of their location.

2.1.1 General Jurisdiction- The person's contacts with the forum state are sufficiently continuous and systematic.

2.1.2 Specific Jurisdiction- It refers to the power of the applicable court with respect to a cause of action based upon some set of minimum contacts with the forum state that relate to that cause of action.

2.2 Subject-matter Jurisdiction- An authority confined to a bounded space, including all those present therein and events which occur there.

2.3 Territorial Jurisdiction- An authority over the subject of the legal dispute.

2.4 Exclusive or Concurrent Jurisdiction- Where a court has exclusive jurisdiction over a territory or a subject-matter; it is the only court that is authorized to address that matter. Where a court has concurrent or shared jurisdiction, more than one court can adjudicate the matter.

2.5 Jurisdiction in Civil Matters

The problem of jurisdiction in contractual obligations is an important aspect. In the internet contract, if the parties can be properly identified and they chose a national law by which they would be governed, the forum will be that state.

Hence, in the case *CompuServe, Inc. v. Patterson*, 89 F 3d 1257 (6th Cir 1996) the parties decided to be governed by the law of State of Ohio. The court in Ohio did not hesitate to decide that case. But the laws with regards to jurisdiction when parties do not choose the forum, State are still not clear.

Indian jurisprudence regarding jurisdiction over the internet is almost non-existent. Except on a few occasions, foreign judgments are binding on Indian courts. This position of law assumes importance when foreign judgment in internet case is to be enforced. The main argument on behalf of defendant would be that a foreign court has no jurisdiction to try the matter. He might argue that judgment was passed in absentia of party and was not enforceable. However, the Indian judiciary has held that these reasons are not valid.

Based on this principle, the Indian court would not have any doubtfulness to enforce any foreign judgments.

In India, a suit in respect of immovable property or in respect of movable property that is under attachment, is required to be instituted in the court within whose local jurisdiction, the subject-matter is situated. In an internet case, when the property is situated in a foreign country, this provision becomes irrelevant. Another provision state that a suit for the compensation of the wrong done to person or to movable property, may be instituted either at the place of residence of the defendant or at the place where the wrong was committed.

2.6 Jurisdiction in Criminal Matters

Since Internet is everywhere, the commission of a crime can take place anywhere on the internet due to this the internet user finds himself, the subject matter of the jurisdiction of many countries for a single act. Occasionally this may lead to a situation where a person is subject on extradition request from many countries. Ordinarily the jurisdiction of a court relates to the place where the offence is committed. This is based on the English Common Law position that all crimes committed in the courts with whose jurisdiction even a part of the offence was committed have a jurisdiction to try the matter. This will result in a situation, where the prosecutors of many jurisdictions have a choice of forum as to the trial of offences. Sections 177 to sections 189 of Criminal Procedure Code deal with the jurisdiction issue in criminal matters. Inland is tried by a court within whose local jurisdiction the crime was committed. In case of several local areas where the offence was committed or continues, be tried by the court in whose local jurisdiction crime was committed or accused is found. If the offence is committed by a person outside India, person maybe dealt in such offence has been committed in India. If the crime is committed by a person, not being Indian citizen, on any ship or aircraft registered in India, he may be dealt with in respect of such offence as if it had been committed at any place within India at which he may be found

2.7 Jurisdiction based on Online Contract

Online contracts come with 'terms of service' agreements and disclaimers. These agreements impose restrictions on the users regarding the choice of law and forum selection. *Bremen v. Zapata Off-Shore Co. (1972)*-

"Such clauses (forum selection) are prima facie valid and should be enforced unless enforcement is shown by the resisting party to be 'unreasonable' under the circumstances."

In the case *Ramanathan Chettier v. Somasundaram Chettier*, AIR 1964, Madras 527, the principle of "*lex foris*" (the law of the court or forum) is applicable with full force in all matters of procedure. No rule of procedure of foreign law is recognised. India accepts the established principle of private international law that the law of the forum in which the legal proceedings are instituted governs all matters of procedure.

2.8 Jurisdiction based on Location of a Web Server

Asserting personal jurisdiction based on the defendant's use of IT infrastructure of a service provider, located in the forum state, to host its website may also compel the forum state to exercise its jurisdiction over such defendant.

2.9 Jurisdiction based on Code of Civil Procedure

Personal Jurisdiction is governed by the Code of Civil Procedure, 1908 in the Indian Courts. The CPC does not treat private international law disputes differently.

In the Code of Civil Procedure, the basis for deciding territorial jurisdiction stays the same as any domestic dispute, but to decide on the subject matter jurisdiction of a suits the code has specified a distinction on which type of suits will be governed under it, these are -

- a) For suits on immovable property,
- b) For suits on movable property and wrongs to persons, and
- c) For any other category of suits, Section 20 is a “default rule” as it provides for categories of suits not covered in the above two categories.

Under the Code of Civil Procedure, two conditions might arise that will decide the jurisdiction of the matter so impugned. The first situation is where the contract contains a choice of court clause and the second situation where there is no predetermined agreed forum. In the first situation obviously, the court so agreed upon by the contracting parties will have the jurisdiction, but Section 20 of the Code of Civil Procedure will come to the rescue. Section 20 of the Code of Civil Procedure states that a court can exercise jurisdiction in actions involving persons where:

- a) the defendant, or each of the defendants where there are more than one, at the time of the commencement of the suit, and voluntarily resides, or carries on business, or personally works for work,
- b) any of the defendants, where there are more than one, at the time of commencement of the suit actually and voluntarily resides, or carries on business, or personally works for gain, provided that in such case with the leave of the court has been obtained or the defendants who do not reside or carry on business, or personally work for gain, as aforesaid, acquiesce in such institution, and
- c) The cause of section wholly or partly arises.

3. INTERNATIONAL PERSPECTIVE OF JURISDICTION ISSUES IN CYBERSPACE

3.1 Based on perspective, the issue of jurisdiction divided into two types-

3.1.1 Prescriptive Jurisdiction- Any State has its own laws in respect of any matters it chooses. A State may legislate for any matter irrespective of where it occurs, or the nationality of the persons involved. It is unlimited jurisdiction.

3.1.2 Enforcement Jurisdiction- Jurisdiction of any State within its own territory is presumptively absolute over all matters and persons situated there.

Section 75 of the Information Technology Act, 2000.

3.2 Territorial Principle- It is applicable for those granted immunity under international law. A case *S.S. Lotus (France v. Turkey)*, PCIJ Ser A (1927) decided by The Permanent Court of International Justice is a good example. (Singh, Justice Yatindra, 2016).

3.2.1 Objective Territorial Principle- where a State exercises its jurisdiction over all activities within its territory, even though some element constituting the crime or civil wrong took place elsewhere.

3.2.2 Subjective Territorial principle- Where a State asserts its jurisdiction over matters commencing in its territory, even though the final event may have occurred elsewhere.

3.3 Nationality Principle- A State may exercise jurisdiction over its own nationals irrespective of the place where the relevant acts occurred. A State may even assume extra-territorial jurisdiction.

3.4 Protective Principle- It is applicable when State's national security or subject matter of public interest is in issue. The case *Attorney-General of the Government of Israel v. Eichmann, 36 ILR (1961)* is a suitable example in this regard.

3.5 Passive Personality Principle- The citizen of one country, when he visits another country, takes with him for his protection the law of his own country and subjects those, with whom he comes into contract, to the operation of that law.

In the Case *United States v. Yunis, 681 F Supp 896 (1988)*, the US District Court, District of Columbia explained this principle.

3.6 Universality Principle- A State has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern. Act of terrorism, attacks on or hijacking of aircraft, genocide, war crimes etc.

4. JURISDICTIONAL ISSUES AS THE CHALLENGE FOR THE REAL SPACE LAW

The effectiveness of a judicial system rests on bedrock of regulations. Regulations define every aspect of a judicial system's functioning. But a court must have jurisdiction, venue and appropriate service of process to hear a case and render an effective judgment. The many issues on internet cannot be managed by existing principles of jurisdiction. The court all over the world is facing difficulty in finding out solutions to the internet litigations. The most difficult question is regarding the jurisdiction. In the physical world, the principles for establishing applicable law and deciding jurisdiction in cross-border litigations were established many years ago. But because of the special characteristics of the internet, these rules cannot be applied in fixing jurisdiction of internet cases. (Sharma, Vakul, 2013)

5. JUDICIAL OUTLOOK IN CYBERSPACE JURISDICTION

In the case *Pres-Kapp, Inc v. System One, Direct Access, Inc, 636 so. zd 1351 (Fla. Dist. ct. App. 1994)*, (Sharma, Vakul, 2013) the decision involved electronic contracts through a computerized airline reservation system. The plaintiff owned and operated a computerized

airline reservation system. The computer base for the system, as well as, the plaintiff's main billing office, was in Florida. A branch business office operated out of New York. The defendant, a New York Corporation, owned and operated a travel office in New York. The two parties negotiated a lease contract in New York, the breach of which was the subject of the lawsuit. The court found only two contracts between the defendant and the forum State Florida, namely that the defendant forwarded lease payments to a billing office in Miami and the defendant's computers made electronic contracts with the plaintiff's computer base in Florida.

Citing the case *Burger King Corp. v. Rudzewicz*, (1985) 471 US 462 in this case, the court found that a contract with an out-of-state party alone could not establish jurisdiction. That left only the electronic contracts with a computer database for the court to consider. The Florida Appeals court held that electronic contacts with a computer database located in the Forum State were insufficient to establish personal jurisdiction. Thus, the defendant did not purposefully avail himself of Florida's jurisdiction and the first prong of the test failed. The court warned about the unfairness of allowing jurisdiction where the only contract is between computers.

In the case *Panavision v. Toeppen*, 938 F. Supp. 616 (C.D. Cal. 1996), the plaintiff, a Delaware Limited partnership with its principal place of business in Los Angeles, California, succeeded in establishing jurisdiction in California over an individual residing in Illinois by relying chiefly upon the effects test. The case focused on a domain name dispute, involving an alleged "Cyber Squatter", who occupied Panavision's domain name with the intent of extorting money from it. The court ruled based on the effects test that personal jurisdiction was proper. (Sharma, Vakul, 2013)

6. JURISDICTION UNDER INFORMATION TECHNOLOGY ACT, 2000

Section 61 of IT Act, 2000 provides that the civil courts have no jurisdiction in the matters of cyberspace. Section 61 of IT Act, 2000 reads as

"61. Civil court not to have jurisdiction- No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act."

Section 13 of IT Act, 2000 provides that if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business.

The sub-sections (3) (4) and (5) deal with the cause of action clause, which is of significance in Internet transactions to determine the jurisdiction.

Section 13 (3) discusses that save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business and is deemed to be received at the place where the addressee has his place of business. Section 13 (4) of IT Act, 2000 highlights that the provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under the sub-section (3).

Section 13 (5) of IT Act, 2000 discusses that for the purposes of this section -

- a. If the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

- b. If the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;
- c. "Usual place of residence" in relation to a body corporate, means the place where it is registered.
- d. Section 75 and section 2(2) provides that the act shall apply to an offence committed outside India by any person. (Ahmad, 2008).

The leading Case *State of Tamil Nadu v. Suhas Katti*,(2004) is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. Impugned emails were sent to the victim by the accused via a false email account in name the victim. Because of such posts the victim was receiving exasperating phone calls. Thereafter a complaint was filed by the victim against the accused. The accused was then arrested by the police and it was shocking to find out that the accused was already known to the victim.

The accused was found guilty of offences under sections 469 and 509 of Indian Penal Code and section 67 of Information Technology Act, 2000 and was convicted and sentenced to undergo rigorous imprisonment for two years under section 469 Indian Penal Code and to pay fine of Rs.500/-and for the offence under section 509 Indian Penal Code sentenced to undergo one year simple imprisonment and to pay fine of Rs.500/- and for the offence under section 67 of IT Act, 2000 to undergo rigorous imprisonment for two years and to pay fine of Rs.4000/. All sentences to run concurrently.

Further in the case *Avnish Bajaj v. State (N.C.T.) of Delhi*, 2005(79) DRJ 576, Avnish Bajaj (Appellants), CEO of Baazee.com, an online auction website, was arrested for distributing cyber pornography. The charges stemmed from the fact that someone had sold copies of a pornographic CD through the Baazee.com website.

Section 67 of the Information Technology Act relates to publication of obscene material. It does not relate to transmission of such material. There was no prima facie evidence that Mr. Bajaj directly or indirectly published the pornography and actual obscene video could not be viewed on the website in issue. The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. one lakh each. The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the Court.

Further in the case *Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy & Anr.*,(23 Nov. 2009), the preliminary objection in the present case is the jurisdiction of the Delhi High Court. the defendants' website is interactive and is accessible from anywhere in India, and that "universality, ubiquity, and utility" of the Internet and the World Wide Web, all are indicative that the High Court possessed the jurisdiction to hear the matter.

In the case *Dhodha House v. S.K. Maingi*,2006 (9) SCC 41, the Supreme Court had clearly observed that the presence of the person concerned is not necessary for carrying on business at a place and must only conform with the three conditions:

1. The agent must be a special agent who attends exclusively to the business of the principal,
2. The person acting as agent must be an agent in the strict sense of the term, and

3. That to constitute 'carrying on business at a certain place, the essential part of the business must be performed at that place.

Section 66 A of the Information Technology Act, 2009 was held to be violative of Article 19 (2) of the Constitution of India, 1950 and hence the same was struck down by Hon'ble Supreme Court in *Shreya Singhal v. Union of India* (24th March 2015).

7. CONCLUSION AND SUGGESTIONS

Of all the cases mentioned above, the basic conclusion and suggestions are:

- a) The Indian judiciary has made all the efforts to uphold the fundamental rights of the citizens and ensured balance between individual and societal interest.
- b) The legislation is still not effective enough to combat all the issues that arise where the offenders are using internet as a mode of violating rights of innocent citizens and trying to extract monetary benefits out of such practices.
- c) Many cases are registered wherein the offenders try to extract money by way of cloning the debit/credit cards or by way of data digging. They use the personal information of the victim to hamper his image in the society.
- d) The basic need of the hour is to make masses in general aware about the methods by which they can be subjected to cyber crimes. When people will be aware about the kinds of cyber crime that exist they already will ensure all the safeguards to protect their rights and identities.
- e) The internet is boarder-less. Anyone can obtain information or do business from any part of the world. This is raising legal issues that are required to be dealt with globally.

REFERENCES

- Ahmad, F.,(2008). Cyber Law in India, Pioneer Books, 3rd edition
- Chopra, D., (2003). Cyber Cops, Cyber Criminals, and Internet, Keith.
- Dudeja, V.D, (2003). Information Technology and Cyber Laws, Commonwealth
- Fatima, T.,(2011). Cybercrimes, Eastern Book Company, Ist Edition.
- Issue of jurisdiction under the information technology act' 2000, <https://www.scribd.com/doc/53929521/issue-of-jurisdiction-under-the-information-technology-act-2000>
- Johnson & Post - WordPress.com, <https://yalelawtechdotorg.files.wordpress.com/2011/08/riseofcyberlaw.pdf>
- Paranjape, V., (2010). Cyber Crimes & Law, Central Law Agency
- Singh, Y.,(2016). Cyber Laws, New Delhi, Universal Law Publishing Co. P. Ltd., 6th Edition.
- Sharma, V., (2013). Information Technology Law and practice – Cyber Law and e-Commerce, Universal Law Publishing Co. P. Ltd.,3rd edition, pg. 387.
- Verma, S.K., Mittal R., (2017). Legal Dimensions of Cyberspace, New Delhi, Indian Law Institute.