Jurisdictional Issues in Adjudication of Cyber Crimes

Mr. Justice A. Muhamed Mustaque
High Court of Kerala

What is cyberspace?

- The term “cyberspace”—

  (A) means the interdependent network of information technology infrastructures; and

  (B) includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

- Cyber space is a broad term which includes computers, networks, software, data storage devices, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

- ***Cybercrimes*** can be broadly categorized into two kinds:
  1) Where traditional crimes such as theft, forgery, defmation etc. are committed electronically.
  2) where a computer itself is attacked.

- The Indian Penal Code (**IPC**) and the Information Technology Act, 2000 (**IT Act**) both contain the substantive provisions relating to cybercrimes.

Statutory Framework of Cyber Crimes in India

Some of the penal provisions under the IT Act, 2000 are :

a. Damage to computers/ computer systems- Section 43 of the Act
b. Data theft and Hacking- Sections 66B to 66D of the Act contain provisions pertaining to offences ranging from identity theft to violation of privacy
c. Cyberterrorism- the provision is penalized under Section 66 E of the IT Act
d. Obscenity- Section 67 of the IT Act penalizes publishing or transmitting of obscene material in electronic form.
e. Child pornography or child sexually abusive content – is punishable under Section 67 B of the IT Act.

IPC also contains certain provisions that could extend to cybercrimes, some of which are:

a. Obscenity - u/s. 292 to 294
b. Staking which included cyberstalking - u/s. 354D
c. Cyber frauds - u/s. 420
d. Email spoofing - u/s. 463
e. Defamation through email - u/s.499
f. Various kinds of harassment and intimidation are covered - u/s. 503 to 507

Cyber Jurisdiction- National, Transnational or International

National-

Jurisdiction will be national where:

- the domestic legislation grants jurisdiction to the courts within the country,
- As a national crime, the jurisdiction defines the illegality, who prosecutes the crime, and who eventually punishes individuals who violate this national law,
- Examples of national jurisdiction would be for offences under the IT Act, 2000 where the courts in India would be vested with the appropriate jurisdiction.

Transnational-

- When a crime involves more than one country
- Cyber crimes are very likely to be transnational in nature as a hacker physically present in the USA could hack a computer in London and steal data present on the device.

International-

- Cyber crimes can be international in nature and the distinction between an international and transnational crime can be hard to distinguish.
- However, cyber crimes do not come under the category of “International Crimes” under the Rome Statute for International Criminal Court.

Tests to determine Jurisdiction

Reasons why there could be jurisdictional issues in cybercrimes:

1. Material posted on the internet has worldwide audience;
2. It is easy to move website from one territory to another;
3. A website can be hosted on one area, but directed at users in another geographic location;
4. Parts of a website may be hosted in one area, while other parts of the websites are hosted in another location; and
5. It is not always possible to determine where a website or user is located.

Theories of Jurisdiction

1. Subjective Territoriality-

- Forum state will have jurisdiction if the act took place within territory of the forum state;
- Ex- section 2 of IPC provides for punishment of offences committed within India.

2. Objective Territoriality/ Effects Jurisdiction -

- When the action takes place outside the territory of the forum state, but the primary effect/consequence of that activity is within the forum state;
- Ex- Section 179 of the Code of Criminal Procedure grants jurisdiction to Indian courts based on the effects doctrine.

3. Nationality -

- The right to prescribe a law for an action based on the nationality of the actor;
- Ex- section 4 of the IPC stipulates that the provisions of the Code would also apply to any offence committed by any citizen of India in any place without and beyond India.

4. Passive Nationality –

- Jurisdiction based on nationality of victim

5. Protective Principle -

- Desire of a sovereign to punish actions committed in other places solely because it feels threatened by those actions;
- Victim is usually the government or the sovereign;
- Not a preferred principle of jurisdiction- as at cost of other nation’s sovereignty.

6. Universality Principles-

- Any state to have jurisdiction;
- Pertaining to certain offences- gravity of offence.

Yahoo!, Inc. v. La Ligue Contre Le Racisme

Facts:

- Yahoo!, an American Internet service provider (Delaware corporation), brought a suit in federal district court against La Ligue Contre Le Racisme et L'Antisemitisme ("LICRA") and L'Union des Etudiants Juifs de France ("UEJF") seeking a declaratory judgment that two interim orders by a French court are unrecognizable and unenforceable. The interim orders against Yahoo! and Yahoo! France.

Issue:

- Whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States resident within the United States on the basis that such speech can be accessed by Internet users in that nation?

- The Court held that the principles of comity do not require the United States to permit foreign regulation of speech by a United States resident within the United States on the basis that Internet users in that nation can access such speech.
- “Comity is neither mere courtesy and good will, nor an absolute obligation.”
- “U.S. courts generally recognize foreign judgments as long as enforcement is not contrary to U.S. interests.”
- The Court held that enforcement of the French order directing Yahoo! to prevent French citizens from accessing Nazi items offered for sale by third parties would violate the first amendment rights of Yahoo! and, therefore, cannot be enforced.
- The Court held that Yahoo! has shown that the French order is valid under the laws of France, that it may be enforced with retroactive penalties, and that the ongoing possibility of its enforcement in the United States chills Yahoo!'s First Amendment rights. It held that Yahoo! had also shown that an actual controversy exists and that the threat to its constitutional rights is real and immediate

Microsoft Ireland Case [Microsoft Corp. v. United States]

Facts:

- The case involved certain evidence concerning drug-trafficking stored in the cloud. The magistrate judge hearing the case he issued a warrant directing Microsoft to produce all emails and information associated with an individual customer account.
- The suspect, however, in spite of being a resident of the US, had registered for his account as a resident of Ireland. As per the policy of the company, the emails were stored on a server in Ireland. Subsequently, when confronted with the production order by the judge, the company complied with providing the account information but refused to turn over the emails, arguing that a US judge has no authority to issue a warrant for information stored abroad.
- A federal magistrate judge disagreed with Microsoft and ordered it to turn over the emails. Microsoft appealed the decisions and the case was before the Supreme Court.

- While the case was being heard, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was enacted.
- The CLOUD Act amended the Stored Communications Act (SCA) of 1986 to allow federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.

Extra-territorial Jurisdiction - Cybercrimes

- Section 4 of IPC envisages extra-territorial application of the code where the offence is committed by a citizen of India, or by a person on a ship or aircraft registered in India.
- It also extends jurisdiction of the code to any person in any place without and beyond India committing offence targeting a computer resource located in India.
- Contrasting this with the Informational Technology Act, 2000 where Section 1 (2) states:

> “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 person.”

- Section 75 of the IT Act further states that the Act shall apply to an offence committed outside India by any person if the act constituting the offence *involves a computer, computer system or computer network located in India.*
- Section 75 of the IT Act is wider in ambit than Section 4 (3) IPC as the former would include jurisdiction in case of offences committed abroad which involve a computer, computer system or computer network located in India, and not just where the computer resource targeted is located in India as is the case under IPC.

Corresponding Provisions in CrPC

- **Section 179 :** An act being an offence by reason of anything done and of a consequence ensued, the offence may be inquired into or tried by a court in whose local jurisdiction-
  - ➔ such thing was done; or
  - ➔ the consequence has ensued
- **Section 182 :** Offences of cheating by letters etc. and, cheating and dishonestly inducing delivery of property, may be inquired into or tried by any court within whose local jurisdiction-
  - ➔ the letters were sent or received and
  - ➔ the property was delivered by the person deceived or was received by the accused.

Ajay Agarwal v. Union of India 1993 AIR 1637

- The appellant was a Dubai based NRI who, along with 4 others, conspired and cheated Chandigarh bank and got foreign letters of credit issued through the bank.
- ***Held*****:** There is an illegal act of dishonestly inducing the bank. A foreign national is amenable to jurisdiction under Sections 179 and 182 of CrPC since the offence was committed in Dubai and the consequence ensued in Chandigarh.

Lee Kun Hee & Ors. v. State Of U.P. & Ors 2012 {3} SCC132

- In terms of the agreement, the seller (based in Delhi,India) supplied certain products to the intermediary buyer (based abroad) which was further transferred to ultimate beneficiary (foreign Company). The ultimate beneficiary executed a bill of exchange in favour of the intermediary buyer and the intermediary buyer endorsed the bill of exchange in favour of the seller, towards payment for products. The ultimate beneficiary did not honour its commitment under the bill of exchange.
- The seller carrying its business activities either in Delhi or Ghaziabad, through its sole proprietor filed a criminal complaint before the Magistrate at Ghaziabad, against the ultimate beneficiary.
- The appellants argued that they were of foreign nationality, their residence was outside India, and that they were not present in India when the offence(s) was/were allegedly committed.

- The Supreme Court held that Indian Courts would have jurisdiction and relied upon S. 179 CrPC.

Held:

- The two phrases of Section 179 Cr.P.C. “anything which has been done”, with reference to the offence and “consequence which has ensued” substantially enlarge and magnify the scope of jurisdiction contemplated under Section 179, so as to extend the same over areas contemplated by the two phrases.
- With reference to the facts of this case, the court held that the words “anything which has been done”, would extend to anything which has been done in furtherance of the execution of the agreement.

➔ Applying this interpretation, S.179 can be said to confer jurisdiction to Indian courts w.r.t offences under S. 4(3) IPC and S.75 of IT Act.

- **Section 188**: This provision grants courts in India jurisdiction where an offence is committed outside India, either by:
  - ➔ a citizen of India whether on the high seas or elsewhere; or
  - ➔ by a person, not being such citizen, on any ship or aircraft registered in India,
  - ➔ Corresponding provision of S. 4 of the IPC
  - ➔ However, it does not touch upon the jurisdiction of Indian courts in case of S. 4(3) i.e. where an offence is committed by a person, outside India, targeting a computer resource located in India.
  - ➔ S. 188, therefore, will not apply either in case of S.4(3) of IPC or S. 75 of IT Act, unless the offence is committed by an Indian Citizen.

The Budapest Convention on Cybercrime

- The first international treaty which discusses the Internet and cybercrime.
- It considers the national laws, increasing cooperation among nations and improving investigative techniques;
- Jurisdiction under Article 22 of the Convention allows the country to have jurisdiction if the cyber crime is committed:
  a) In its territory;
  b) On board a ship flying the flag of the country;
  c) On board an aircraft registered under the laws of the country by one of the countries 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

- The Council of Europe, USA, Canada, Japan are some of the signatories of the Convention.
- However, some countries including India are not signatories to the Convention.
- The Convention provides for:
    1. Criminalisation of conduct ranging from illegal access, data and systems interference computer-related scorn and child pornography;
    2. Procedural law tools to make the investigation of cybercrime and the securing of electronic evidence in relation to any crime more effective;
    3. International Police and judicial cooperation on cybercrime and e-evidence

Mutual Legal Assistance Treaties (MLATs)

- MLATs in criminal matters are bilateral treaties, entered between the countries for providing international cooperation and assistance.
- It is a mechanism whereby countries cooperate with one another in order to provide and obtain formal assistance in prevention, suppression, investigation and prosecution of crime.
- It aims to ensure that the criminals do not escape or sabotage the due process of law for want of evidence available in different countries.
- India has entered into MLATs with 42 countries.*
- A request for assistance or information can made by the Central Authority of India to the Central Authority of another country on the request of the Investigating Officer/ Agency under the MLAT.

- MLA requests can be distinguished from Letters of Request u/s. 166A as the latter is issued by the Indian Court on the request of the Investigating Officer or Investigating Agency.*
- India has also signed MoUs with countries on security cooperation which covers prevention of cyber crimes.
- In 2015, India signed an MoU with Germany on Security Cooperation covering areas of border protection, aviation security, cyber crime, illegal migration and counterfeit currency.*
- In 2016, India signed MoUs with Singapore, Malaysia and Japan, relating to Cyber Security to promote cooperation for exchange of knowledge and experience in detection, resolution and prevention of security related incidents between the countries and India.*

IPR in Cyberspace

India TV, Independent News Service Pvt. Ltd. v. India Broadcasting Live

Facts:

- A Hindi news channel “INDIA TV”, launched in March 2004, was run by the plaintiffs. The trademark (INDIA TV) was adopted in 2002.The domain name “indiatv.com” was owned by the plaintiff which was registered in 2003. The channel was made available for live streaming on the said website.
- The Defendants’ hosted the website “www.indiatvlive.com”. The website contained the words “INDIA TV”. The defendants lived in USA.
- Plaintiff filed a case for passing off action in the Delhi High Court to prevent Defendant from using the domain name “www.indiatvlive.com”. While the suit was pending, Defendant filed a case in the US against the plaintiff seeking a declaration of non-infringement of the plaintiff’s mark by Defendant.

Issues Raised:

1. Whether the defendant's activities "have a sufficient connection with the forum state (India)?
2. Whether the cause of action arises out of the defendant's activities within the forum?
3. Whether the exercise of jurisdiction would be reasonable?

- The Defendant’s website had provisions for subscription to its services which could be availed of by residents in India.

Held:

- Defendant intended to target Indians residing in India and expatriate Indians. Since the website of Defendant was launched in India as well as in Los Angeles, Defendant’s company has sufficient connection with India.
- Regarding the “effects test”, since the plaintiff channel was an Indian news channel made for Indian audiences, any harm alleged to have been caused or to arise to the good will, reputation of the plaintiff would be in India.
- Therefore, the Defendant‘s carrying on activities within the jurisdiction of this court has sufficient contacts with the jurisdiction of the court and the claim of the plaintiff has arisen as a consequence of the activities of Defendant within the jurisdiction of this court.

THANK YOU