Jurisdictional Approach towards Cyber Crime in India

Garima Mohan Prasad
Assistant Professor of Law
IILM University, Greater Noida

Abstract

Every state now have extra-territorial jurisdiction to cover the extra-territorial area of issues relating to cyber space the International Trade adopted a Model with named E-Commerce in year 1996 and which was adopted by the General Assembly Resolution too, the General Assembly the asked every state to give its permission so India being its member adopted the Information Technology Act, 2000 to cope up with the increased no of crime in the 20th century.

This paper is divided into five sections-

1. Jurisdictional Approach of Cybercrime and Meaning of jurisdiction
2. Jurisdiction decision on I.T Act
3. Power of police Officers and other officers under the IT Act
4. Conventions on cybercrime
5. Conclusion

Keywords- cybercrime, jurisdiction, IT Act, Convention

Approach of Cybercrime & Meaning of Jurisdiction

Jurisdiction is the authority of a court to hear a case and resolve the matter accordingly which include person, property and subject matter. All sovereign and independent states possess jurisdiction over person and thing within its territorial limit and all causes i.e. civil and criminal arises with this jurisdiction.

Jurisdiction over Internet

The main point regarding jurisdiction is the existence of multiple parties all over the world the parties are just connected to each other through virtual nexus, the main in deciding the jurisdiction whether civil or criminal is done just on two points

- First basis is the place where the defendant reside.
- Second basis is the cause of action i.e. the place where the crime occurred.

However if we talk about the jurisdiction of cyberspace it is very difficult to decide the jurisdiction as there is no geographical boundaries to decide the same the communication between two parties just happen on the basis of internet for example-

If a person sitting in India is communicating with an individual in London and using the software of Canada then the laws of all these three countries can be theoretically used in deciding the jurisdiction so the best way decided to come from such situation was many countries started signing international convention and treaties.

The main theories behind jurisdiction of cybercrime. There are six field mainly on which the cybercrime jurisdiction is decided:-

- **Subjective territoriality**-This one is the most prominent among the six theories of jurisdiction, the substantial legislation of every country quotes that if an cyber activity takes place within the jurisdiction of that state then the person will be liable under the laws of that country same as section 4 of Indian Penal Code.

- **Unprejudiced/ Objective territoriality**-In this type of territoriality jurisdiction the main concept what work is more than where the crime has occurred the place where it has effected most of it, the doctrine what it works here is called the “effect” doctrine foe example if Pakistan has attacked the computer system

of India say some of government organization then the effect will be seen in India and hence section 179 of Crpc work for effect jurisdiction.

- **Nationality-** This type of jurisdiction works if the offence is committed by that person leaving in some other country than their on respective state, same as section-4 of Indian Penal Code works if the offence is committed by India leaving somewhere else other than India.

- **Passive Nationality**- This particular theory is based on the nationality of that citizen when the offender and victim are of the same state then that country has more power in prosecuting such offence.

- **The Protective Principle**-This principle work when the government and the victim are on the same path that means the sovereign or the government is itself responsible for the offence committed, this principle is not preferred as the victim cannot punish itself.

- The last but not the least is the universal jurisdiction in this particular kind of jurisdiction issue like sea piracy, slavery, genocide, air piracy has to be established which means the same law can work for all the nations, article 105 of United Nations on the Law of Sea works means this principle works outside the territory region the state may seize the pirated ship and other person who has committed piracy, further it was stated seizure will decide the amount of penalties imposed and will determine what kind of action has to be taken with regard to aircraft, seizure and can punish the person if found guilty.

Jurisdiction Decision under the Information Technology Act 2000

It has been already discussed the I.T act has been passed to decide the matters on cyber related offences so the I.T Act runs along various forums to decide the particular case like

(I) Adjudicating Officers selected by controller

The controller selects the adjudicating officers and resolved alleged violations of the aforementioned rules and elect geographical location which may exercise jurisdiction, the adjudicating officer hear both the parties and then will decide the “wrong doer” mainly in cybercrime what is decided the person has done a wrongful act it can be harassment, hacking and squatting etc. the qualification of adjudicating officer is decided on the basis of his or experience it can be in both civil orc criminal.

(ii) Cyber Regulations Appellate Tribunal

The government of India can establish Cyber Regulation Appellate Tribunal to specify the “matter” and places pertinent to its jurisdiction which all has been explained in detail under section 48 of the I.T act the main purpose is to decide the case first on the basis of this tribunal then it may be appalled to the Central Board or Adjudicating Officers and the main point is no other can enter fair under the affairs of adjudicating officers under the I.T Act ,2000 or other courts cannot pass injunctions on the decision of appellate tribunal If the parties agrees the decisions of adjudicating officers then no appeal can be filed an appalled can only be filed to the Tribunal within 45 days of the decision by this board.

(iii) Appeal to High Court

Then decision which is rejected by the tribunal can be appealed in the High Court of that state, it must be filed within 60 days after the decision comes from the tribunal.

(iv) Extra-territorial Jurisdiction

Earlier the Information Technology Act was not well versed with the extra territorial jurisdiction but with the amendment in the I.T Act things have changed for example if a person from United States of America hacks the computer sitting in India so maximum the Indian Court can do is passed the degree in favor of the plaintiff but we

cannot punish that U.S citizen so the laws of our country must be strong enough to fight against such cybercrimes.

India's Position

Indian Judiciary is playing an very important role on deciding the jurisdiction according to the provisions section 75 this act apply to an offence committed even outside the territory of India.

The important case laws which elaborate the extra territorial jurisdiction of India are:-

In **Yahoo Inc. vs Akash Arora & Another** this was the first case where the issue related to domain name was decided the second one was the case called Rediff this too was based on deciding the domain.

Jay Jethani and Another vs State Of Haryana on 18 October, 2019[1]

This case was decided recently on 18th October 2019, Jay Jethani was the petitioner in this particular case the petitioner was booked under **section 75** and **section 66 D** of the **I.T Act** by the state of Haryana who was the defendant in this case as per the FIR of the Haryana Police they were running a call center on illegal manner in the building name Vampire Ltd located at **sector 37** Guru gram and the accused are making false calls on the internet but the accused were later released on bail as the allegations made by the police of Guru gram was proved false.

Takhat sinha Ravish Solanki vs Regional Passport Office on 12 December, 2018[2]

In this particular case a writ was filed under **section 226** of the constitution of India where the petitioner has appealed to renew his sons passport petitioner's son was working in Toronto with a private company and was living there for a limited period of time but his passport got expired and when he went to the Indian Embassy in Canada they refused to do so as F.I.R was filed against him in city called Bhuj located in Gujrat

The plaintiff son was charged under **section 504,507,499** and **section 66 & 75** of the **Information Technology Act 2000**, therefore the plaintiff has requested in his writ if his sons passport will renew he will give full support in the investigation process of

[1] Available at "https://indiankanoon.org/doc/86704875/" (visited on 14/11/2022)

[2] "case search on Indian Kanoon website under section75 of the I.T Act"

Gujrat Police, later the court of law gave permission to renew the passport of plaintiff's son.

India has a famous case known as **CBDT case** which has explained the concept of extra territorial jurisdiction in a very broad way, this CBDT is a statutory body in India whose website was hacked by the people sitting in Pakistan after investigating around three years there was no achievement for the investigating officers the main reason was that the attackers were sitting in Pakistan India was helpless in this case as Pakistan was recognizing the hackers and further refer to them as patriots , this situation was not only faced by India but countries from all over the world faces the same scenario.

India after facing such problem on extradition many times decided to amend their act and there came **section 75** of the act which states person sitting anywhere outside India has done such an offence will be treated accordingly with the **Indian Cyber laws**.

India now promised to be an action spot and will be changing itself accordingly with the technology if we compare India with other **Asia Pacific Countries** then we can see India is more likely to be the one who has tackled very tricky cybercrime issues within the world.

The I.T amended act has been able to solve the problem of jurisdiction arising through cybercrimes like hacking, stalking, squatting committing through anywhere in the world. "**Section 81** of **IT Act** declares law to be special law and states that the provisions of this law shall prevail over anything inconsistent contained therewith in any other law currently in force in India."

Indian Penal Code

Amendment has been added in **section 4** of the **Indian Penal Code** which has strengthen the issue of jurisdiction under the **Information Technology Act 2000**. The sub **section 3** of section four states that this particular provision apply to any person who live at any place beyond India committing offence like targeting a computer resource in India.

Civil Procedure Code

The **Civil Procedure code** decides the jurisdiction on the following basis[3]:-

- Firstly the place of residence
- Secondly where the cause of action has taken place but in cyber world it is totally different here the cause of action can be more than one for example the website can be accessed from anywhere in the global world.

[3] Civil Procedure Code 1908

Power of Police and other Officers under the I.T Act 2000

The police too have given special power under section 78 of the Information Technology Act after all the police have the huge responsibility of investigation it is carefully stated a person not below the rank of inspector can investigate in this particular case other than **section 78**, **section 80** also deals with the power of police it states that a police officer not below the rank of an inspector, or any other officer of the State Government or the central government authorized by the central government to enter any public place and search and arrest without warrant so the main ingredient of **section 80 (1)** are :-

- The power to enter any public place and search and arrest without warrant any person found therein is vested only to police officer but not below the rank of inspector.
- The power can be exercised very much at public place as per **section 80** it can be any public place which is reachable to the police
- The police officer must be sure that a person at public place is suspected and has committed offence under the **I.T Act 2000**.

So it is clear from the study that cyberspace has no jurisdictional boundaries and is an ever-growing in exponential and dynamic space the best example of the same is that of using E-commerce websites a person can purchase anything from one place of the world to another by just sitting at a particular place so such situation therefore give rise to one question which jurisdiction has to applied so to solve such kind of problem international treaties and conventions have been formed and the other thing what is attached to this is the cyber laws should not only contain procedural law but must have substantial laws too as cyber laws just not means offence related to computer but it contains offensive criminal activities attached to it.

Judicial Retort of United States of America

As we say the country United States of America is the most powerful country in the whole wide world and so it has large amount of laws as compared to India on criminal offences according to the United States Department of Justice said that the punishment for cybercrime offenders shall only be punished only with the USSG guidelines.

- **United States Personal Jurisdiction in cyber space**

The Courts in United States have been borrowing the principle of personal jurisdiction and has extended it to the cyberspace jurisdiction the jurisdiction theory that was earlier used for just physical setting is now used for website too, the websites represents a virtual model the point which can be taken for consideration is the geographical location of user or website owner and website server, further the website are classified in two types interactive website and Passive website under interactive website as the name suggest passive websites are those who just provide a mere information whereas interactive website provides more than a information and is interactive basis.

In **United States vs Pirello** is one of the landmark case of United States the defendant was fraudulently selling computer later he was punished by the nine circuit rule of the **USSG guidelines**. The other case which defines extra territorial jurisdiction is United Nation VS Ivanov in this particular case under the computer fraud and abuse case act was explained regarding the extraterritorial jurisdiction the accused was charged for illegally retrieving the computer system of a web hosting service under the computer Fraud and Abuse Act of United Nation of America the plea put forward by the plaintiff was that during the commission of an offence he was in Russia so how can be this applicable on the plaintiff later it was decided by the court that he can be prosecuted under the interstate commerce of the Act. The other case where there was charged for advertising pornographic material on the internet. The main point under this act is that a person can be punished for extraterritorial jurisdiction.

In the famous **Yahoo France case** the judicial thinking on jurisdiction was redefined, this particular case redefined the principle of jurisdiction for example if a foreign country delivers a judgment which is against the legal entity of a particular country suppose Country A then that judgement would not be liable for the whole country in every kind of matter this case has kept sovereignty of the other state in mind and then have given their decision after this many countries adopted this principle

Judicial Retort of United Kingdom

With the increment in use of technology and Internet United Kingdom has made many diverse cyber laws and the first case that was registered was R VS Gold in year

1998,the United Kingdom country decided to make special law called the Computer Misuse Act 1990 for the purpose of combating cyber terrorism in the global world.

Conventions on Cybercrime

The first conventions on cybercrime was held in Budapest on 23rd November 2001where many countries become it signatories, this particular convention mainly deals with offences like infringement of copyright, child pornography and computer related offences.

The main motive behind this convention was to set a common principal policy aimed for the protection of society at large by adopting preventive measure in order to deal with cyber offences, it has made cybercrime an extraditable offence and had made the offences punishable by hearing both sides of the parties.

- **Cyber Crime and the Issue of Extradition**

The conventions on Cybercrime has made this an extraditable offence and is punishable under the law in both constricting parties by imprisonment for more than a year or through penalty. This Convention Article-24 is against the rule of double criminality which states that a person can be punished both by requested state and requesting state.

This particular conventions has made all the cybercrime as extraditable in nature or in other words we can say that search, seizure and investigations of all cyber offences has been made added in these conventions so that no country can suffer in order to prosecute their cyber criminals.

In **Rambhu Saxena Vs State**[4] the jest of this case was if the treaty does not include a particular offence under extradition but can authorize Indian Government to allow extradition for some additional offence by adding new clause.

Hence the type of **Cyber Jurisdiction** has been defined

- Civil matter jurisdiction of Cybercrime
- Criminal matter jurisdiction of Cybercrime
- Cyber Jurisdiction in International Cases

Civil Matter Jurisdiction of Cybercrime

[4] AIR 1950 SC 1888

- **In Bensusan Restaurant Corp vs King**

This case is the famous case of **America New York state**, the court of New York lacked the jurisdiction in this particular case as alleged by the plaintiff that the defendant was the operator in Columbia and has infringed his trademark whereas the point put forward by the defendant was that it was created in Missouri and focused on the residents of that state only and just the consumers buying ticket does not infringed the right of trademark.

In Zippo Mfg. v Zippo Dot.com

The court here stated the difference between active website and passive website as stated the passive website are those which only share information and there is no sufficient ground on what basis jurisdiction will be decided whereas in active website the users of that particular websites enter into a contract and knowingly active websites comes into field of personal jurisdiction here the defendant has registered its website as zippo news.com and has many subscribers of that website mainly in Pennsylvania the plaintiff said the defendant has stolen its domain name as it was used by him but the court held that in this particular case it has personal jurisdiction and entity incidence on internet.

Criminal Jurisdiction of Cybercrime

Firstly the cyber use of internet jurisdiction was only in case of civil matters but now with the famous case US vs Thomas jurisdiction in criminal matters too become a major problem, the defendant used to run a news bulletin which was only accessed by people having id and password on that particular website which was launched in 1991.The court held that whether the website was using the obscene material will be decided on how much bad impact has it put in the society further the argument put forward by the defendant was that the jurisdiction must be decided on geographical location and the law must be put of that country only.

Cyber Jurisdiction impact on international cases

In Core Vent Corp V. Nobel Industries[5]

[5] AB, 11 F 3d 484 (9th circ 1993)

In Care Vent Corp. v. Nobel Industries the clash was between California Corp the (plaintiff) and five Swedish citizens and three Americans citizens (defendants) for publishing articles containing false and misleading comparison between Core Vent Corp. and Nobel Parma's Dental Implants. The appellate Court of California allowed the jurisdiction will be decided on the basis of rules framed in United States Constitution, further it was also stated it will be decided with three tests

- Whether the nonresident has entered into the contract with the resident of that country for some or the other kind of privilege.
- Whether the claim formed is due to the some activities of the Defendant
- Whether the exercise of jurisdiction will be providing substantial justice or not.

In another case name **Playboy Enterprises Inc. vs. Chuckleberry Publishing Inc.**[6]

The defendant has a particular pay website which was even used by the people living in US the customer used to pay in order to access the website with its own login id and password generated but the United States court held that they have enough jurisdiction from selling the magazine of the plaintiff in their native country.

In R vs Oliphant [7]

He was living in Paris and have written wrong data for the firm in London so the main question for the court here arises two countries must except cross border jurisdiction and a person can be liable with "effect" jurisdiction which the crime which effected the State.

In Simpson V. State [8]

In this case the victim was in a small boat near the Georgia side of the Savannath river whereas Simpson who was the defendant made several shoots on the plaintiff but the shot does not take place on the correct spot The Supreme Court of Georgia held that jurisdiction attached with these circumstances and that Simpson could properly be prosecuted in Georgia even though the defendant was clearly in another state at the

[6] 939 F. Supp. 1032 (S.D.N.Y. 1996).

[7] [1905]2 K. B. 67

[8] [92 Ga.41.17S.E.984(1893)]

time of shooting. The location of the victim and the place where the bullets landed established the basis for the decision.

Convention on Jurisdiction of cybercrime

The Cybercrime convention of the Council of Europe has prescribed the issue of jurisdiction under Article 22, and further requires every nation should adopt prominent legislative measures to make jurisdiction over any country established under the convention when the offence is committed in its territory this particular convention has provide nationality and subjective but has not worked in the “effect” kind of jurisdiction.

Conclusion

We can say that computer adds a new dimension to cyber law and thus presenting many laws for its enforcement there must be new technological data for investigation since if the investigation is not done properly then the whole process will go in vain. It is important to enact useful legislations that can be sufficiently stop the bad use of internet or we can say the abasements of cyber world sometimes cyber laws does not differentiate between cyber jurisdiction or criminal jurisdictions but the law should be such that with provide clear view of the jurisdiction issue.

Bibliography

1. Internet Source

- https://www.webopedia.com/DidYouKnow/Hardware_Software/FiveGenerations.asp
- https://www.newsfirst.lk/2019/05/19/cyber-attack-on-several-sl-websites/
- www.mondaq.com
- https://indiankanoon.org/doc/86704875/
- http://crime-in-crisis.com/en/wp-content/uploads/2017/06/74-SYKIOTOU-KOURAKIS-FS_Final_Draft_26.4.17.pdf
- https://shodhganga.inflibnet.ac.in/jspui/

2. Books

- An introduction to cyber law by Dr. J. P Mishra
- Cyber law by Pawan Duggal