RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF JURIDICAL SCIENCES

COURSE:BA.LL.B

Semester : VIII th

SUBJECT: Cyber Law

SUBJECT CODE:BAL-805

NAME OF FACULTY: Dr.Puja Paul Srivastava

RAMA UNIVERSITY

Lecture-29

LECTURE 29: Investigation and jurisdiction over cyber crimes.

The invention of computer and computer networks has made the life easier and above all the internet is proved to be a cherry on the cake. The usage internet of technology has turned the world into a global village. Now a days anyone can access the resources on internet within a blink of an eye from anywhere in the world. On one side where everything seems to be smooth and easy, the other side of this cyberspace culture highlights the complex issues and vulnerability regarding cyber crimes.

The article specifically focuses on the issue of determining the jurisdiction of Indian courts while dealing with cases of cyberspace. The article gives the idea of certain provisions that deals with the jurisdiction issue in the country with help of case laws. The objectives of international conventions and participation of India has also been discussed further. Moreover, the article also mentions few suggestions for resolving the confusion of cyber jurisdiction.

Introduction

Today a world cannot be imagined without the internet connectivity which has become a basic necessity of a human being. This global network has made the life easier through its immense contribution in communication and information sharing. It is playing a pivotal role in almost every field of life either its education, business, politics, medicine, infrastructure or science and technology.

The advent of internet culture gave the concept of a virtual world called as Cyber space which is basically a virtual environment created by interconnected computers and computer networks on internet without any boundary of distance and physical limitations. 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.

Just like every coin has two sides the same goes with the cyberspace technologies which has its own pros and cons, there is no doubt that it has simplified our life to a greater extent but the dark side of the story reveals that in recent years the computer technology and cyber space has became an invitation to cyber threats.

The issue of cyber threat involves the criminal activities ranging from minor electronic crimes to more serious offences such as illegal gambling, theft of personal information, cyber bulling, cyber stalking, cyber defamation, web jacking, data diddling etc however these offences are not only the concern but it also raises the question of jurisdiction in order to deal with the cases of such cyber-crimes. It is evident that cyber space has no restriction of a physical boundary therefore it becomes convenient for criminals to access the system from any part of the world with the means of computer or any electronic devices.

For instance, A person sitting in china could break into a bank's host computer in India and transfer millions of Rupees to another bank in Switzerland, all within a blink of an eye. Only thing he would require to do this is a computer and a cell phone device. Once the crime has been committed the confusion of jurisdiction arises as to where the complaint should be logged for the trial of such cases. This is because of the disparities among the laws of different countries to deal with cyber crime cases.

Jurisdiction over cyber crime and national laws

Jurisdiction is the power or authority of the court to hear and determine the cause and adjudicate upon the matter that are litigated before it or the power of the court to take cognizance of the matter brought before it but when it comes to determine the jurisdiction in context of cyber space it becomes strenuous part of law.

In common parlance Jurisdictions is of two types:

Subject jurisdiction allows the court to decide cases of a particular category and to check whether the claim is actionable in the court where the case has been filed.

Personal jurisdiction allows a court to decide on matters related to citizens or people of its territory, the person having some connection to that territory, irrespective of where the person is presently located. Every state

exercises the personal jurisdiction over the people within its territory

The concept of jurisdiction can be understood in a better way with reference to section 15 to 20 of code of civil procedure (1908) which talks about the place of suing or the subject matter jurisdiction and section 20 of this code specifically speaks about any other category of suit which is not covered in sec 15 to 19 of the code.

Section 20 serves important ingredients for the purpose of institution of other suit in a court within the local limits of whose jurisdiction'[1]:
the defendant or each of the defendants resides, or carries on business, or personally works for gain at the time of the commencement of suit.
Any of the defendants, where there are more than one defendants resides, or carries on business, or personally works for gain at the time of the commencement of suit provided that in such cases either the leave of the court is given, or the defendants who do not reside, or carry on business, or personally works for gain, as aforesaid, acquiesce in such institution or,
the cause of action wholly or partially arises.

However, this section doesn't seem to be fit in virtual world. The issue with the cyber space jurisdiction is the presence of multiple parties across various part of the globe who only have virtual connections among them therefore we cannot have a clear idea about the parties and the place of suing so that the jurisdiction of the court could be determined to try such cases.

The substantive source of cyber law in India is the Information Technology Act, 2000 (IT Act) which came into force on 17 October 2000. The objective of the Act is to provide legal recognition to e- commerce and to facilitate storage of electronic records with the Government.

The IT Act also penalizes various cybercrimes and provides strict punishments. In pursuant to this there are certain provision under this act which renders the idea of jurisdiction of court for the trial of cases pertaining cyber crimes in India as well as outside India.

Such provisions of IT Act are as follows:
Sec 1 specifies the extent of the application of this act. It states that:[2]
(2) 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.
Sec 75 deals with the provisions of the act to apply for offences or contravention committed outside India. It states that[3]:
subject to the provision of sub section (2), the provision of this act shall also apply to any offence or contravention committed outside India by any person irrespective of his nationality.
For the purpose 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.
Comment: The above sections sec1(2) and sec 75 of the IT Act applies to any offence or contravention committed in India as well as outside India. The application of this act outside India is empowered by invoking the power of extra territorial jurisdiction of nation It is immaterial to the fact that whether the offender is citizen of India or not and whether the crime has been committed inside or outside of India because it applies to any person irrespective of their nationality if he harms or tries to the computer, computer system or network located in India either by operating in India or from any part of the world.

Sec 46 of the Act renders power to adjudicate in case of contravention of any provision of this act and for the purpose adjudging it provides for the appointment of adjudicating officer who is vested with the powers of civil courts which are conferred on the Cyber Appellate Tribunal

Sec (48) of the act provides for the Establishment of Cyber Appellate Tribunal[4].
(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

Comment- This tribunal is established by the government under this Act and the government itself decides the matters and places as to where the tribunal would exercise its jurisdiction. It is considered as the first appellate

tribunal where the appeal from the orders of control board or the adjudicating officers is preferred. Further any person aggrieved by the decision of appellate tribunal may prefer appeal in High Court within sixty days from the date of communication of such decision or order.

The Information Technology Act 2000 seems exhaustive when it comes to adjudicate the matter where the parties are Indian citizen and the offence or any contravention has been committed in India as the Indian Courts follow the Principle of lex foris that means the law of the country but it still creates confusion in order to exercise its extra territorial jurisdiction where the offence has been committed outside India or by any non-citizen.

For instance, if an American citizen damaged the reputation of one of the Indian Politician by publishing lewd comments through the social media and the aggrieved person approached to Indian court for the justice. It is obvious that IT act, 2000 provides for extra territorial jurisdiction but the issue arises here that how far would it be effective to bring the American citizen to India to be prosecuted for cyber defamation as the IT Act is not applicable to the American citizen.

Apart of IT Act 2000, there are other relevant legislation under Indian laws that gives the authority to India Courts to adjudicate the matters related to cyber-crimes such as:
Sec 3 and 4 of Indian penal code 1882 also deals with the extra territorial jurisdiction of Indian courts[5].

Section 188 of CrPC 1973 provides that even if a citizen of India outside the country commits the offence, the same is subject to the jurisdiction of courts in India. Section 178 deals with the crime or part of it committed in India and Section 179 deals with the consequences of crime in Indian Territory[6].

Relevant cases laws:
SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra[7]
This is a case related to cyber defamation. This is first case of its kind from India. In this case, the defendant was an employee of the plaintiff's company who used to send derogatory, obscene, vulgar, and abusive emails to his employers and also to different subsidiaries of the said company all over the world. The motive behind sending those emails was to malign the reputation of the company and its Managing Director all over the world.

The High Court of Delhi assumed jurisdiction over a matter of defamation of reputation of corporate through e-mails. An ex-parte injunction was granted by the court.

SIL Import v. Exim Aides Silk Importers[8]
In this case the court successfully highlighted the need of interpretation of the statute by judiciary in the light of technological advancement that has occurred so far . Until there is specific legislation in regard to the jurisdiction of the Indian Courts with respect to Internet disputes, or unless India is a signatory to an International Treaty under which the jurisdiction of the national courts and circumstances under which they can be exercised are spelt out, the Indian courts will have to give a wide interpretation to the existing statutes, for exercising Internet disputes.

Impresario Entertainment & Hospitality Pvt. Ltd. vs S&D Hospitality [9]
Facts – in this case the plaintiff's company offers restaurant services which has its registered office in Mumbai and is carrying its business in New Delhi and a restaurant under the name and style of 'SOCIAL' which it has trademark and has various branches as well. The plaintiff came to know about the defendant's restaurant in Hyderabad under the name 'SOCIAL MONKEY.

Also, it has a popular beverage by the name A GAME OF SLING and the defendant has named a beverage as Hyderabad Sling which is identical or deceptively similar to the plaintiff's beverage. Both these outlets had entered into contract with websites like Zomato and Dine Out and so the information of both, along with menu and contact info was made available on the websites of Zomato and Dine Out.

Therefore, issue before the Delhi High Court was whether it had the jurisdiction to adjudicate upon the matter?

The Hon'ble Court also observed that for the purposes of a passing off or an infringement action (where the plaintiff is not located within the jurisdiction of the court), the injury on the plaintiffs business, goodwill or reputation within the forum state as a result of the Defendant's website being accessed in the forum state would must be shown. Therefore, the court held that mere interactivity of the website in the forum State did not attract its jurisdiction.

Earlier similar view was given in the case of Banyan Tree Holding (P) Limited v. A. Murali Reddy and Anr[10] wherein the court held that a passive website, with no intention to specifically target audiences outside the State where the host of the website is located, cannot vest the forum court with jurisdiction.

India and international convention over cyber jurisdiction:
Convention on Cyber crime, 2001 also known as the Budapest Convention, is the first international treaty which discusses about the Internet and cybercrime by considering national laws, increasing cooperation among nations and improving investigative techniques. It was signed by the Council of Europe in Strasbourg, France, Canada, Japan, Philippines, South Africa and the United States. However, countries like India and Brazil have declined to adopt the Convention on the grounds that they didn't participate in its drafting but due to increasing incident of cyber crimes India has been reconsidering its stand on the convention since 2018.

Article 22 The Convention on Cyber Crime, 2001 allows the country to have jurisdiction if the cyber crime is committed [11]:
In its territory;
On board a ship flying the flag of the country;
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.

United Nations Convention against Transnational Organized Crime (UNTOC):
This treaty was adopted by resolution of the UN General Assembly in November 2000. India being a signatory to this joined in 2002. UNTOC is also known as the Palermo Convention, under this the state parties are obliged to enact domestic criminal offences that target organised criminal groups and to adopt new frameworks for extradition, mutual legal assistance, and law enforcement cooperation. Although the treaty does not explicitly address cyber-crime, its provisions are highly relevant[12]. In pursuant to this treaty Indian Parliament enacted the Information Technology Act 2000.

Recommendations:
There is a need for unique law which can be applied to determine the jurisdiction in cases of cyber crimes. A law must be developed at international level in nexus with the countries which are in vulnerable position to cyber threats.
India must become an active participant and signatory to conventions and treaties which aims to curb cyber crimes and provide security to cyber space.
In order to determine the jurisdiction of court the loopholes in laws should be identified and the necessary amendments must be brought to widen the scope of adjudication.
The parliament must formulate the laws regarding the extradition policies.

SELF-TEST QUESTIONS

S.NO	Question	Option (a)	Option (b)
1.			
2.			
3.			
4.			
5.			

Answers: 1-(),2-(), 3-(),4-(),5-()