Provisions Concerning Extra Territorial Jurisdiction Under the Information Technology Act, 2000

-Sparsh Jain

1st year student of Symbiosis Law School, Noida.

Abstract

The Internet and the growing cyber space are a major part of our lives these days. Online transactions, the data being stored online and to ensure data privacy are of growing importance to governments, enterprises and even consumers throughout the world. With the constant growth and expansion of cyberspace it has given rise to many critical opportunities involving lack of security and data being stolen giving rise to increasing cyber crimes these days. The internet does not have any physical limitations and geographical boundaries therefore these crimes can take place from anywhere in the world by someone with access to the bare minimum of resources. The purpose of this article is to analyze the provisions of extra territorial jurisdiction under the Information Technology Act of 2000 and what are the issues that we need to address to come through with an effective way to exercise the jurisdiction of the Indian courts or any courts for a fact outside their territory and reduce cybercrime.

Introduction

Today the entire world can be considered as one whole community. The entire world is connected with the help of the internet. The internet has made our life easier by simplifying the communication as well as information sharing process. The internet created a cyberspace which is basically a virtual environment created by interconnected computers and computer networks online without any boundary of distance and physical limitations.

Although the internet and the continuous developments in the online world have made our life so much easier but on the other hand it has given rise to increasing cases of cybercrimes or cyber offences.

What are cyber offences?

Cyber Offences refers to offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modem telecommunications network such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS). There are numerous types of cyber-crime involving hacking, identity theft, malicious viruses, phishing attacks, IPR violations, cyber terrorism, frauds, pornography, spam, etc. One such offence of Child pornography was newly introduced in Section 67 B of the information technology act in an attempt to address the issue of child pornography[1].

The internet does not have any territorial boundaries to which it can be restrained nor does it have any physical boundaries. Cybercrimes covers all sorts of criminal activities be it minor electronic crime to more serious offences. Activities such as theft of personal information, cyber bullying, cyber stalking, or even illegal gambling, etc. fall under the definition of cybercrime 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 cyberspace has no restriction of a physical boundary therefore

[1] The Information Technology Act, 2000, §67(B).

it becomes convenient for criminals to access the system from any part of the world with the means of computer or any electronic devices[2].

For instance, A person sitting in Bangladesh 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. He would require the bare minimum like a computer and a cell phone device to carry out this offence after which the main confusion of jurisdiction arises as to where the complaint should be filed for the trial of such cases in which multiple jurisdictions are involved.

What is jurisdiction and what role does it play in tackling cyber crime?

Jurisdiction is the power or authority of the court to hear and determine the cause and adjudicate upon the matter that is litigated before it or the power of the court to make legal decisions and judgements regarding a particular situation.

Certifying jurisdiction in respect to cyber space becomes a task which requires great efforts. In cyber jurisdiction multiple parties are involved across various parts of the globe and the only thing common among them is the virtual connection they have with each other online via the internet therefore we cannot have a clear idea about the parties and the place where they can be held liable thereby making it difficult to determine the jurisdiction under which the accused will be held liable.

Why is there a growing need of cyber laws in India for the past few years and to equip the judiciary with enough extra-territorial powers to tackle cyber crime?

Computer crimes had not emerged as a major problem area of the law enforcement agencies in India until recently. The main reason for low incidence of computer-related crimes in India was that computerization of banks and other financial institutions were still in early stages. Further, the networking of computers had not yet taken place in any big way in the sensitive sectors which could be vulnerable to theft and alteration of data. But as the process of computerization has now picked

[2] Kirty Ranjan, *Analysis of Cyber Jurisdiction in India*, Legal Services India, www.legalserviceindia.com/legal/article-3329-analysis-of-cyber-jurisdiction-in-india.html.

up, significant increase in computer crime is expected in the near future. Cyber-crime has now become a reality in India. Difficult to detect, seldom repeated and even more difficult to prove, computer related crime lacks traditional paper audit trail, is away from conventional policing and requires specialists with a sound understanding of computer technology. Furthermore, as the company on its path to become a superpower in the next few years the government is pushing for digitalisation of the economy for a smooth and better functioning process to be followed and with the country posed to enter the information superhighway for industry and banks networked, the realization of the dangers and threats is are finally being realised. The major areas of concern, which are highly vulnerable to computer crimes, include critical infrastructures like banks and other financial institutions, telecommunications, airlines, railways, power sector and other crucial departments of both the Government of India and numerous States etc.[3]

The government of India has a job to protect the citizens from any threats that may lead to the hindrance in the functioning of the day-to-day life of the people. Just like we fear war, with the advancements in the online cyberspace the biggest threat to a nation is cyber warfare. Everything is now stored online on secured servers so if anyone were to hack or gain unauthorised access to such documents then give rise to a threat to national security. Therefore, the government needs to be equipped with the adequate methods to prevent such crimes as well as to punish the people that try to engage in such malicious activities.

Extra territorial jurisdiction takes into account any offence which is committed by a citizen of India or even by any person on a ship or aircraft registered in India or by any person who targets a computer resource located in India, beyond the territories of the Indian Subcontinent.

Problems and shortcomings in the legal field regarding the provisions of extra territorial jurisdiction with special emphasis on India

[3] Mr. Kush Kalra, *Emergence of Cyber Crimes: A challenge for the New Millennium,* docs.manupatra.in/newsline/articles/Upload/4730150C-4A12-4EBA-8CAF-F1146FDD5657.pdf.

One of the main problems in tackling cyber-crimes is the disparities among the laws of different countries and their ways to deal with cyber-crimes.

Suppose Mr. X commits an offence from his home computer targeting a network in India. Therefore, he might or might not be held liable cause something which is considered as an offence in India might not be an offence in his home country thereby leaving the Indian government and the Indian courts incapable of carrying out their jurisdiction and litigating against the crimes committed by the accused.

A variety of National laws that apply to foreign people or companies outside the territorial boundaries of a country are intended to have extraterritorial effects. Some laws are intentionally made to have extraterritorial effects aiming to ensure that people do not become victims of law-breakers from outside their jurisdictions. We have established that the governments have a responsibility to protect their citizens from illegality, but the global and cross-border nature of the Internet can create conflicts arising from activities that are legal in one country but might be illegal in another. In the early 2000s, as the Internet became popular and commercialized, the Yahoo case highlighted the challenges of Internet regulation. The American search and listings company, Yahoo, was forced to stop advertising Nazi memorabilia for sale in France, and its executives were faced with criminal charges.[4]

However, many Internet-related laws and international frameworks only regulated where absolutely necessary to promote commerce, and promoted openness and innovation in the development of the networks. For example, the idea of 'mere conduit' – where network operators are not liable for the content of traffic – is found in the laws of many countries, including the European E-Commerce Directive of 2000. Governments took a light regulatory touch domestically and coordinated regionally and internationally to allow the Internet to flourish.

In the cyber world every State should have its national law having extraterritorial jurisdiction to tackle the situation and challenges of extraterritorial nature present in the cyberspace environment as there were no international regulations and instruments relating to cyber jurisdiction around 1995. Therefore, the United Nations Commission on International Trade Law adopted a model law on e-commerce in 1996 which was adopted by the General Assembly. The general assembly recommended

[4] *Licra v. Yahoo!*, High Court of France, core.ac.uk/download/pdf/235401821.pdf.

that all States should give favourable consideration to the said model law on commerce. India being signatory to said model law enacted The Information Technology Act, 2000 to make law in tune with the said model law.

Section 1 of the information technology act states that:

The provisions in section 1 (2) 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.[5]

Section 75 of the Information technology Act also addresses this issue stating that the provisions of the information technology act shall apply to any offence

- 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.
- 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.[6]

Since there are no physical boundaries and limitations for a cyberspace the information technology act is empowered with the help of extraterritorial jurisdiction to develop a safe online environment and to hold the people committing cyber crimes accountable for their actions irrespective of their nationality.

One of the biggest drawbacks of the IT Act, 2000, is that it doesn't take into account the jurisdiction of the Courts in the cyber world. It means the present law of jurisdiction of the physical world is applicable to the cyber world as well. In India, Sections 15 till 20 of the Indian Civil Procedure Code (C.P.C), 1908, and Sections 177 till 188 of the Indian Criminal Procedure Code, 1973, deal with civil and criminal jurisdiction respectively.[7] Under the Cr.P.C., territorial jurisdiction depends upon the

[5] The Information Technology Act, 2000, §1(2).
[6] The Information Technology Act, 2000, §75.
[7] Supra note 3.

place where offence or part of the offence is committed. Under the C.P.C, the territorial jurisdiction is based upon:

- place of residence of the defendant[8], and
- place where cause of action arises. But in the cyber world there may be more than one place of cause of action, such as place of cause of action may be a place where a Website is accessed, or place where a server is located or place from where an electronic record is sent or place where an electronic record is received.[9]

However, the IT Act, 2000, time and place of dispatch and receipt of electronic record is defined.

Section 75 of the Information Technology Act, 2000 extends jurisdiction of Indian Courts to an offence or contravention committed outside India by any person irrespective of his nationality. Further, this law is to 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.[10]

For example, Mr. Z, an Australian national, residing in the USA, gains unauthorized access to a computer located in China and deletes information. Mr. Z has used a computer located in India to gain unauthorized access. Mr. Z will be liable under the provisions of the IT Act, 2000.

The main difference between the Indian Penal Code and the IT Act, 2000 with regard to extraterritorial jurisdiction, can be demonstrated by the following example.

If a foreign national let's say Patrick Lehman, say from Germany legitimately procures weapons from India and uses the same for committing a criminal act in Germany or any other country in the world then she would not be liable for any offence in India as per the Indian Penal Code. However, if Patrick were to use a computer located in India to hack the German government's website or commit any other offence under the IT Act, 2000, then she will be liable for that offence in India.

[8] The Indian Civil Procedure Code, §15 to §20.
[9] The Indian Civil Procedure Code, 1908, §177 to §188.
[10] Supra note 6.

The problems with the differences in the laws in various countries and various provisions arises when we look at the practical aspect of such provisions such as that of mere conduit which might be applicable in one country but might not be enforceable in the other.

Mere conduit simply is a law which enforces that the network operators are not liable for the content of traffic. This provision has been adopted by various countries such as the United States of America and can even be found in the European E-Commerce Directive of 2000. The governments generally maintain a light regulatory touch domestically and coordinate accordingly at an international level for the internet to flourish at a global level.

One of the things that we can use to tackle the issue of cybercrime in respect with extra territorial jurisdiction would be the strengthening of the capacity of lawmakers and the judiciary.[11] The judiciaries in many developing countries including India need to be trained in the area of cyber laws. Legal issues around e-commerce are still relatively new. We can't tackle a problem if we don't understand each and every aspect of it therefore to convince and prosecute the accused in their country, we have to be educated with each and every technicality there is that could help us or either strong arm us when we bring it up at an international level.

Moreover, the international committee should develop a professional and strict procedure of action to be taken when such crimes are committed by someone from their country or anyone else around the court and comply with the other country to bring the accused forward rather than sheltering him on a technicality.

Conclusion

Majority of the crimes committed that fall under extra territorial jurisdiction relate to data privacy and personal data of individuals as well as of big corporations that are targeted by hackers from all over the globe. In the global economy, accumulating personal data of the consumers has become a driving

[11] Note by the UNCTAD secretariat, *Cyberlaws and regulations for enhancing e-commerce: Case studies and lessons learned*, United Nations Conference on Trade and Development, unctad.org/system/files/official-document/ciiem5d2_en.pdf.

fuel for much commercial activity online. This data is used by the corporations in understanding as well as influencing consumer behaviour for commercial profit but if fallen into the wrong hands may further raise concerns about the stability of the network that we have online, something which we all access everyday very easily every now and then.[12]

The nature of the internet is such that it is ever evolving and its use is increasing day by day and the internet has no limits, no physical boundaries. Therefore, before going ahead into this new era of digitalisation the international community should take necessary steps to formulate a confined set of international laws addressing the problems of each and every country. An international body such as the United Nations should assume the lead once again not only encouraging member states to formulate national laws in this crucial area but also come out immediately with a model law to facilitate such a move and bring about uniformity in national laws covering cyber jurisdiction.

There is much work to be done in the implementation of the laws. Laws are made for everything but the problem arises due to the lack of proper implementation. One thing might sound good on paper but might not be practical in the real world thereby leading to loopholes being generated. The internet is constantly expanding and is dynamic in nature and therefore the laws governing it should be implemented according to the situations prevailing in the real world. This will provide us an ability to curb cybercrime while simultaneously allowing the online cyber space to grow and evolve and to be used by the billions of people around the world safely without the customers feeling vulnerable and exposed to malicious activities thereby creating a safe environment after all.

[12] Ibid.