International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Crimes in India: An Analysis

Gurvinder Singh

Assistant Professor, Department of Law, Chaudhary Devi Lal University Sirsa, Haryana

ABSTRACT

In today's techno-savvy environment, the internet is treated as a research and information sharing tool. Since the number of internet users is on the rise, it gives birth to Cyber Crimes. All issues relating to Cyber Crime or internet crime are dealt with through Cyber Law. So, to get the remedy against Cyber Crime, the need for Cyber-Law arises. Cyber Law is important in a country like India where the internet is used to a large extent. The law is enacted to save people and organizations from Cyber Crime and other internet-related crimes. It protects the privacy of every individual and organization. Before the enactment of Cyber Law no specific law existed in India to deal with Cyber Crime. As per rules and regulations of the Cyber Law, a person who commits Cyber Crime is liable to get punishment. If anyone violates and breaks the provisions of the law, then it allows another person or organization to take legal action against that person. The requirement of Cyber Law can arise as under: Nowadays as all the transactions related to shares are done in Demat form, anyone who is associated with these transactions requires internet and protection under Cyber Law in case of any fraudulent transaction. Most of the companies in India keep their official data in electronic form. To avoid the misuse of such data, a company can need the assistance of this law. Due to the rapid growth of technology, various Government forms like ITR return, Service tax returns are filled in electronic form. Anyone can by hacking the government portal sites easily misuse those forms. Only under Cyber Law, you are eligible to get remedy against this type of fraud. People are using credit cards and debit cards for shopping purposes. However, some frauds through the internet clone those credit cards and debit cards. Card cloning is a technique where someone with the help of the internet easily obtains your card details. With the help of Cyber Law, you can easily trace such criminals. Digital Signatures and e-contracts are the most common methods of transacting business. Anyone who is associated with such digital Signatures and e-contracts can easily make fraud by misusing them.

Keywords: *Computer Networks, Resources, Cyberspace, Cyber Crime, Cyber Jurisdiction, , Storage Devices Technology etc.*

Introduction

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. 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.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. At the end of the 20th century and the beginning of the 21st century, the use of computers and mobile phones saw a significant rise. Later, with its increasing utility, the rise of the internet began in the 1990s. In the last 15-16 years, the role of social media, online payments, education, gaming, communication, movies, search engines have eventually become an essential part of everybody's day to day life, and so did the misuse of it have increased. The real reason behind this is the lack of stringent laws, awareness, lacunas in the safety and privacy of a user and etc. Cyberlaw also governs cyberspace. "Cyberspace refers to the virtual computer world, and more specifically, an electronic medium that is used to facilitate online communication. Cyberspace typically involves a large computer network made up of many worldwide computer sub-networks that employ TCP/IP protocol to aid in communication and data exchange activities.The ambit of Cyber law is so vast that its jurisdiction in a case involving various countries is very difficult to ascertain. A website, app, product, content in one country may be legal but illegal in another, the parties may be residents or non-residents, which makes this concept all the more complex. Cyber law's jurisdiction depends on the kind of cyber-crime and the location from which it has been done.

Defining "Cyber Crimes"

The term "cyber-crimes" is not defined in any statute or rulebook. The word "cyber" is slang for anything relating to computers, information technology, internet and virtual reality. Therefore, it stands to reason that "cyber-crimes" are offences relating to computers, information technology, internet and virtual reality.

In common parlance Jurisdictions is of two types:

1. 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.
2. 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.

Such provisions of IT Act are as follows

- Sec 1 specifies the extent of the application of this act
- 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.
- 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 contravention involves a computer, computer system or computer network located in India
- Article 22 The Convention on Cyber Crime, 2001 allows the country to have jurisdiction if the cyber crime is committed .

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.

Crimes against individuals –These are committed against individuals or their properties. Some examples are:

- ✓ Email harassment
- ✓ Cyber-stalking
- ✓ Spreading obscene material

- ✓ Unauthorized access or control over the computer system
- ✓ Indecent exposure
- ✓ Spoofing via email
- ✓ Fraud and also cheating
- ✓ Further, crimes against individual property like computer vandalism and transmitting a virus. Also, trespassing online and intellectual property-related crimes. Further, internet time thefts are also included.

Crimes against organizations – Some examples of cyber crimes against organizations are:

- ✓ Possessing unauthorized information
- ✓ Cyber terrorism against a government organization
- ✓ Distributing pirated software

Crimes against society – Some examples of crimes against society are:

- ✓ Polluting the youth through indecent exposure
- ✓ Trafficking
- ✓ Financial crimes
- ✓ Selling illegal articles
- ✓ Online Gambling
- ✓ Forgery

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.

Objectives

- ✓ Grant legal recognition to E-Transactions
- ✓ Provide legal recognition to Digital Signatures for authentication Facilitate E-Filing of data and information
- ✓ Allow Electronic storage of data
- ✓ Grant recognition to maintenance of books of accounts in Electronic Form

Cyber Laws of India

In Simple way we can say that cyber crime is unlawful acts wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information

Technology Act, 2000

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could transform itself into an all pervading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the

anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

This section applies if any person, without the permission of the owner or the person in charge of a computer, system, or network

- Accesses such computer, network or system.
- Copies, downloads or extracts any data or information from such computer, network or system (this also includes the information or data stored in a removable storage medium).
- Also, introduces or causes any computer containment or virus into such computer, network or system.
- Further, he damages any computer, system or data or any other programs residing in them.
- Disrupts or causes disruption of any such computer, system or network.
- Also, denies or causes the denial of access to an authorized person to such computer, system or network.
- Provides any assistance to anyone to facilitate access to such a computer, system or network contrary to the provisions of the Act and its rules.
- Also, charges the services availed of by one person to the account of another by tampering with such computer, system or network.

Compounding of Offences

As per Section 77-A of the IT Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if −

- The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR
- Offence affects the socio -economic conditions of the country; OR
- Offence has been committed against a child below the age of 18 years; OR
- Offence has been committed against a woman.
- The person alleged of an offence under this Act may file an application for compounding in the Court. The offence will then be pending for trial and the provisions of Sections 265-B and 265-C of Cr. P.C. shall apply.

Conclusion

Cyber-crime mainly involves activities that use internet and computers as a tool to extract private information of an individual either directly or indirectly and disclosing it on online platforms without the person's consent or illegally with the aim of degrading the reputation or causing mental or physical harm. With the advancement in technology a steep increase in the rate of cyber-crimes has been observed. With the increase of dependency on cyberspace internet crimes committed against women have also increased. This is mainly because around more than half of the online users are not fully aware of the functioning of online platforms, they are ignorant towards technological advancements and have minimal adequate training and education. Thus, cybercrime has emerged as a major challenge for the law enforcement agencies of different countries in order to protect women and children who are harassed and abused for voyeuristic pleasures. Women are commonly targeted for cyber stalking, cyber pornography, impersonation etc. India is one of the few countries which has enacted the IT Act 2000 to deal with issues pertaining to cyber-crimes in order to protect the women from exploitation by vicious predators however this act doesn't address some of the gravest dangers to the security of the women and issues involving women are still growing immensely.The increasing incidents of cyber crime has a detrimental effect in cyber space which in turn posses a threat to national security as well. History of legislation shows that it is almost impossible to eradicate the crime from the virtual world even if the necessary precautions and cyber security measures have been taken. The dawn of cyber laws in India started with the boom in globalization and computerization in India. The number of cyber-crimes registered each year in India is shocking and it is only getting worse. This is because the pool of gullible prey for cyber conmen has shot up with India going digital. This calls for a basic understanding of the laws that govern the cyber space in India.The Cyber Laws in India or the Information Technology Act, 2000 was amended in 2008 to include cyber-crimes related to banking and financial transactions. With the adoption of the IT Act, India is now one of the few countries in the world that have a separate law to deal with IT issues and crimes. This has now paved the way for incredible growth in the fields of e-commerce and internet transactions which has, in turn, resulted in advanced economic growth.Regardless, the implementation of the Act along with its counterpart, the IT Rules, has been successful in tackling cyber-crimes so far. With the ever-growing world of new technology and expanding cyberspace, we aren't yet aware of what kind of cyber-crimes may arise. cyber law is

the appropriate law to provide a remedy against cyber crime. At present, people who commit cyber-crime offenses think twice about the cyber law, before committing any such offenses. The law helps in decreasing the rate of cybercrime offenses.

References

www.tigweb.org/actiontools/projects/download/4926.doc

https://www.tutorialspoint.com/information_security-cyberlaw/introduction.html

https://www.slideshare.net/bharadwajchetan/anintroduction-to-cyber-law-it-act-2000-india

http://www.academia.edu/7781826/impact_of_social_media_on_society_and_cyber_law

https://cybercrime.org.za/definition

http://vikaspedia.in/education/Digital%20Litercy/information-security/cyber-laws

https://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I5-0374.pdf

http://searchsecurity.techtarget.com/definition/emailspoofing

http://www.helplinelaw.com/employment-criminaland-labour/CDII/cyber-defamation-in-india.html

http://ccasociety.com/what-is-irc-crime/

http://searchsecurity.techtarget.com/definition/denialof-service

http://niiconsulting.com/checkmate/2014/06/it-act2000-penalties-offences-with-case-studies/

http://www.cyberlawsindia.net/cyber-india.html

https://en.wikipedia.org/wiki/Information_Technology_Act,_2000

https://www.ijarcsse.com/docs/papers/Volume_5/8_August2015/V5I8-0156.pdf