UNDERSTANDING THE CONCEPT OF CYBER CRIMES IN INDIA VIS-A-VIS CYBER LAWS OF USA

Ms Jyoti Jain & Ms Rashmi Chaudhary

1st Author Jyoti Jain- Research Scholar, Ph.D (Law), Jagannath University, Haryana

2nd Author Rashmi Chaudhary- Assistant Professor, Jagannath University, Haryana

ABSTRACT

With the development of computer technology and internet, the cyber crime becomes one of the most intricate and complex issues in the cyber space. USA is the birthplace of internet and experience the first computer related crime in the year 1969[1]. Cyber space has become a place to do all sorts of activities which are prohibited by law. It is being used for gambling, trafficking in human organs, pornography, hacking, infringing copyright, terrorism, violating etc. So, the cyber crimes affect the whole world at large. There is need of laws governing fast paced cyber crimes. Thus, the present paper is an attempt to compare the Indian present status of cyber legislation with the legislations of USA for exploring the deficiencies and inadequacies of Indian Cyber Laws.

I. Introduction

Internet has created a virtual world without any boundary the virtual space in which the information technology mediated communication and actions are taken place is generally referred to as cyber space. Nowadays, social networking sites have become very popular. These sites have provided a space to go their feelings get new and connect with old friends[2]. The evolution of information technology gave birth to cyber space wherein internet provides equal opportunities to all the people to access information, data storage, analyze etc. with the use of high technology.[3] Some Persons exploit the Internet and other network communications for their own benefit which are international in scope. Now situation is becoming more alarming; Cyber crime is an upcoming and is talk of the town in every society. Theoretically and practically this is a new subject for researchers and is growing exponentially. Though lot of work has been done but endless has to be go because the invention or up gradation of new technology leads to the technical crime i.e. the digital or we can say the cyber crime or e-crime. This is because every day a new technique is being developed for doing the cyber crime and

[1] Talat Fatima, Cyber Crimes, 2011 at p. 45

[2] David Decary Hetu and Carlo Morselli, "Gang Presence in Social Network Sites", *International Journal of Cyber Criminology,* vol. 5 No. 2, July- Dec., 2011, p. 876, *available at:* http:// www.cybercrimejournal.com/ davidcarlo2011julyijcc.pdf (visited on Jan. 8, 2019)

[3] Farooq Ahmad, Cyber Law in India, 2008 at p. 367

many times we are not having the proper investigating method/ model/ technique to tackle that newly cyber crime.[4]

The socio-economic and cultural facets of life have been tremendously affected owing to the rise of globalization. The cyberspace has been a blessing to human civilization[5]. The main task of the Internet is to connect the people around the world with the desire to know about the indispensable human nature which led to the unearthing of the cyber world. Societies and their inhabitants into Knowledge Networkers who are more informed of the events happening locally and globally. Their actions are based on the strong foundation of knowledge which is universal, objective, timely and retrieved from various sources.[6]

Comparatively some organizations have identified organized cyber criminal networks as its most potential cyber security threat and some are ready to defend such security threats. The digital world is increasingly intertwined with the traditional offline world and therefore safety in cyberspace has become a prerequisite for a well-functioning society. A secure cyberspace means a cyberspace where (and from where) no crime is committed. [7]

II. Concept of Cyber Crime

The term *Cyber* denotes the cyber space i.e. virtual space and it means the informational space modelled through computer, in which various objects or symbol images of information exist. Therefore, it is the place where the computer programs work and data is processed[8]. Cyber crimes are nothing but crimes of the real world perpetuated in the medium of computer and hence there is no difference in defining a crime in cyber world and real world. Only the medium of crime is different. [9]

Cybercrime is "international" or "transnational" – there are 'no cyber-borders between countries'. [10] Computer crime, cyber crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is source, tool, target or place of crime as well as traditional crime through the use of computers like child pornography, Internet Fraud. In addition to cyber crime, there is also 'computer supported crime' which covers the use of computers by criminals for communication and document or data storage. [11]

Cyber crime may be defined as "any illegal act fostered or facilitated by a computer, whether the computer

---

[4] Ajeet Singh Poonia, "Cyber Crimes: Challenges and its Classification", *International Journal of Emerging Trend & Technology in Computer Science*, vol. 3, No. 6, at 119 (Nov.- Dec. 2014).

[5] Tanaya Saha and Akanchs Srivastava, "Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of victimization, *International Journal of Cyber Criminology*, vol. 8 No. 1, at 57-58 (Jan.- June, 2014), available at: http://www.cybercrimejournal.com/sahasrivastavatalijcc2014vol8issue1.pdf (visited on March 6, 2019)

[6] Justice T. Ch. Surya Rao, "Cyber laws – Challenges for the 21st Century, "Anuddra Law Times, 2004, at 20

[7] Rutger Leukfeldt, Sander Veenstra, et.al., "High Volume Cyber Crime and the Organization of the Police: The Results of Two empirical Studies in the Netherlands", *International Journal of Cyber Criminology*, vol. 7 No. 1, at 1 (Jan.- June, 2013), available at: http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf

[8] Jyoti Rattan, *Cyber Laws & Information Technology*, 2014 at 215

[9] D. Latha, "Jurisdiction Issues in Cybercrimes", *Law Weekly Journal*, vol.4 at 86 (2008), *available at* www.scconline.com, (visited on June 25, 2019)

[10] Guillaume Lovet Fortinet, "Fighting Cybercrime: Technical, Juridical and Ethical Challenges", *Virus Bulletin Conference*, (2009)

[11] D. Latha, Jurisdiction Issues in Cybercrimes, *Law Weekly Journal*, vol.4 at 85 (2008), *available at:* www.scconline.com, (visited on June 25, 2019)

is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime."[12] An online dictionary defines "cybercrime" as "a crime committed on a computer network."[13] Cybercrimes can be plainly defined as "crimes directed at a computer or a computer system."[14] But the complex nature of cybercrimes cannot be sufficiently expressed in such simple and limited terms.[15] According to Pavan Duggal, Cybercrime refers to all activities done with criminal intent in cyberspace or using the medium of internet. These could be either the criminal activities in the conventional sense or activities, newly evolved with the growth of the new medium. Any activities which basically offend human sensibilities can be included in the ambit of cybercrimes.[16]

III. Indian Cyber Crime Legislations

Parliament of India has passed the first legislation in the year 2000, i.e, Information Technology Act. Chapter XI of the IT Act, 2000 under the heading of 'offences' deals with the various types of offences which are committed in the electronic form or concerning with computer, computer system and computer networks. Further IT Act, 2000 was amended in 2008. Section 66(A) was added by the 2008 amendment which deals with an offence to send offensive message. An offence to receive stolen computer resource is also added under section 66(B). Sections 66(C), 66(D), 66(E) and 66(F) were inserted to declare identity theft, cheating, privacy in cyber space, video voyeurism and cyber terrorism. Section 67-A, 67-B and 67- C were also added which provides punishment for obscenity and child pornography etc. Information technology Act 2000 further amends the Indian Penal Code 1860, the Indian Evidence Act, 1872, the Bankers Books Evidence Act, 1891 and the Reserve Bank of India Act. The Indian Judiciary played an important role in handling cyber crimes in India.

IV. USA Cyber Crimes Laws

The USA has enacted various federal and state laws for the protection of computer, computer network from various cyber crimes. The Wire Fraud Statute was the first law to prosecute the computer criminals in USA[17]. This was an effective statute as it was to overcome defrauding to obtain money, property by false representation or promise; modus operandi being radio or television communication, signs or signals.[18] The Computer Fraud and Abuse Act (CFAA) was enacted by the congress as an amendment of the existing computer fraud law which says that a person is guilty of an offence if he causes a computer to perform any function with intent to secure access to any programme or data held in any computer or he access to secure in unauthorized, and he knows at the time when he cause the computer to perform the function that is the case.[19] Then after Data Protection Act, 1998 was enacted which also control the use and storage of persona data or information relating to individuals. In

---

[12] Sameer Hinduja, "Computer crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future", *International Journal of Cyber Criminology*, Vol. 1, No. 1, January, 2007, *available at:* http://cybercrimejournal.com/sameer.pdf (visited on Feb. 22. 2018).

[13] *available at:* http://scholarly commons.law.northwestern.edu/cgi/viewcontent.cgi?article=7260&context=jclc (visited on Feb. 13, 2019)

[14] Peter Stephenson, *Investigating Computer – Related Crime*, 2000 at p. 3.

[15] *Talt Fatima,* Cyber Crimes, 2011, at p.89

[16] Pawan Duggal, *Cyberlaw- The Indian Perspective*, 2002 at p. 256.

[17] Rajlakshmi Wagh, Comparative Analysis of Trends of Cyber Crimes Law in U.S.A and India. Available at http//technical, cloud-journals .com/index.ph.p//1jacsit//articles/ view/tech-160 (visited on April 12,2019)

[18] Ibid.

[19] Section 1 (i) of The Computer Fraud and Abuse Act, 1998

USA, there are two child pornography laws, that is, the Child Pornography Prevention Act, 1996 and Child Online Protection Act, 1998. The Communication Decency Act, 1996 has been passed to protect the minors from pornography.

In USA almost every state has laws dealing with cyber stalking. US passed the federal laws on cyber squatting which is known as Anti Cyber Squatting Consumer Protection Act, 1999. To stop trade secret misappropriation the National Stolen Property Act and Virgina Internet Policy Act comprising of 7 bills have been passed.

There is large no. of cyber laws passed and amended in USA. The United States Legal system more technology savvy and specialized to tackle the various crimes.

V. Comparative Analysis

In cyber world every state should have its national law having extraterritorial jurisdiction to cover extraterritorial character of cyberspace activity as there is no international instrument relating to cyber jurisdiction. Covering this aspect among others, the UN Commission on International Trade Law adopted a model law on E-Commerce in 1996 which was adopted by the General Assembly by its Resolution. The General Assembly recommended that all states should give favourable consideration to the said model law on commerce. India being the signatory to said Model Law enacted The Information Technology Act, 2000 to make law in tune with the said Model Law. [20]

Jurisdiction under the IT Act is prescribed under sections 1 (2) and 75, which are to be read along with the relevant provisions of the Indian Penal Code, 1860 . Section 1(2) of the IT Act, 2000 provides for the jurisdiction of Indian courts in cyber crimes and contravention. IT Act is silent on the point of the State of Jammu Kashmir, which means that the IT Act extends over the State of Jammu Kashmir. This section provides the extra-territorial jurisdiction over offence or contraventions committed against any computer, computer system and computer network located in India.

In USA, a number of traditional principles relating to jurisdiction are being interpreted in the light of borderless world of cyberspace, jurisdictional problems remain a thorny issue and many experts are of opinion that mere availability of a website is not enough to establish minimum contact to entrench the cyber criminal. [21] In torts matters, the *lex loci delicti*, or the rule that the place in which the injury occurred is the place of trying the case, was followed. But now, the ever expanding boundaries of the internet have, both in civil and criminal matters, exposed the defendant to universal jurisdiction. The question that is often asked whether a defendant who neither ever went out of his jurisdiction nor intended to do so, would rightly be subjected to multiple or foreign jurisdictions and applicable law? [22] In *rem*, jurisdiction might apply to the assertion of claims for jurisdiction based on e-mail storage box or stored file that is located on a computer server in the forum jurisdiction. [23]

---

[20] Jyoti Rattan, *Cyber Laws & Information Technology*, 2014, at p.346
[21] Talat Fatima, *Cyber Crimes*, 2011, at p.457
[22] F. Lawrence Street and Mark P. Grant, *Law of the Internet*, 2004, at pp.3-8
[23] Shaffer v. Heitner, 433 US 186: 53 L Ed 2d 683 (1997)

In both the countries the term "cyber crime" has not been defined while the various authors in the respective countries have attempted to define it. There is no statutory definition exists in both the countries yet. The term 'cyber crime, or 'cyber offence' is neither defined nor this expression is used under the Information Technology Act, 2000 which was further amended in 2008. In fact, the Indian Penal Code, 1860 also does not use the term 'cyber crime' at any point even after its amendment by the Information Technology (Amendment) Act, 2008.

The US have not provided any formal categorisation of cyber crimes while in India the cyber crimes are given under Chapter XI of the Information Technology Act, 2000 under the heading of 'Offences' which deals with the various types of offences

In India, before the amendment made by the Information Technology (Amendment) Act, 2008, the offence covered under section 66 was 'Hacking with Computer System'. But now hacking is replaced by 'Computer related offences'. Under section 66 hacking becomes an offence only when it is committed dishonestly or fraudulently under section 43 the Act. Because before such amendment it was a plain and simple offence with the remedy of compensation and damages only, in that section, here it is the same act but with a criminal intention thus making it a criminal offence. We can also say that if any person cause a computer resource to perform a function with dishonest or fraudulent intent to secure access, knowing that the access he intends to secure is unauthorized then that person is liable under this section.

In the United State of America Computer Fraud and Abuse Act, 1986 deals with the offence of 'Hacking' which is per se illegal only with respect to computers used exclusively by the Government of the United States. Hacking to all other computers, for instance, those used non exclusively by the federal government, including computers containing national security records, and those containing financial and credit records require some further act or damage to occur in order for criminal penalties to apply. [24] Other Acts like Data Protection Act, 1998 has been passed to control the use and storage of personal data or information relating to individuals under § 1030 and the Spyware Control and Privacy Protection Act, 2000 is such an Act to prevent and control hacking in the USA.[25]

In *Briggs v. State of Maryland case,* [26] the US Court held that the statute of the state of Maryland that criminalizes unauthorized access to computers was intended to prohibit use of computers by those not authorized to do so in the first place, and may not be used to criminalize the activities of employees who use employers' computer system beyond the scope of their authority to do so.

In India, there was no specific section under the originally IT Act, 2000 under which sending of threatening emails, which may cause harassment, anxiety nuisance and terror or which may seek to promote instability, have been made a penal offence. Cyber war and cyber terrorism do not find any mention in the Indian Cyber law. But now the Information Technology (Amendment) Act 2008 for the first time made the provision for cyber

[24] Tonya L. Putnam and David D. Elliott, "International Responses to Cyber Crime", *University of Petroleum and Energy Studies Review 1*, at 39-40 (1999), available at: http://www.hoover.org/sites/default/files/ uploads/documents/0817999825_35.pdf (visited on March 6, 2019)

[25] M. Dasgupta, Cyber Crime in India- A Comparative Study, 2009 at p.74

[26] 348 MD.470 (1998) USA

terrorism and defines it in section 66F which provides for punishment for cyber terrorism which provide the highest punishment under this Act. Clause 1(A) of this section deals with cyber terrorism that directly affects or threatens to affects the people with the purpose to threaten the unity and integrity or security of the nation and to fill the terror into the mind of the peoples. Clause 1(B) of this section deals with cyber terrorism that directly affects the State by unauthorized access to restricted information, data or computer database. In 2008, serial blasts in Ahmadabad, Delhi, Jaipur and Banglore are the live examples of the cyber terrorism in India. In 2008 attack on Mumbai Taj Hotel which is also known as 26/11 and the Varanasi blast in 2010 had the trails of cyber terrorism. The main purpose of the cyber terrorist is to gather the restricted information and to spread terror by cyber communications method for disruption of national security, unity, integrity and peace etc.[27]

In the USA, the Computer Fraud and Abuse Act, 1986 has been passed which was further amended in 1994 and 1996. But after Sep. 11, 2001, an attack on World Trade Centre and Pentagon, the USA passed the Patriot Act, 2001 and recognised hacking as cyber terrorism and for the first time defines the term "cyber terrorism". It provides that if any person who causes unauthorized damage to a protected computer by either knowingly causing the transmission of a program, information, code, or command, or intentionally and unauthorizedly accessing a protected computer shall be liable to punishment.

In India, the IT Act, 2000 was deficient in dealing with obscenity before amendment by IT Amendment Act, 2008. It has reformed the Indian law of obscenity to a greater extent. Now, the Information Technology Act, 2000 after amendment states that storing or private viewing of pornography is legal as it does not specifically restrict it. On the other hand transmitting or publishing the pornographic material is illegal. There are some sections of Information Technology Act, 2000 which prohibit cyber pornography with certain exceptions to Section 67 & 67A. The combined effect of sections 66 E, 67, 67A and 67 B is to differentiates between cyber pornography, child pornography and mainstream pornography and to bring the online pornography within the legal regime.

State of Tamil Nadu v. Suhas Katti[28] is a landmark case which is considered to be the first case of conviction under section 67 of Information Technology Act in India which makes this section is of the historical importance. In this case, some defamatory, obscene and annoying messages were posted about the victim on a yahoo messaging group which resulted in annoying phone calls to her. She filed the FIR and the accused was found guilty under the investigation and was convicted under section 469, 509 of IPC and section 67 of Information Technology Act.

In USA, there are two child pornography laws i.e. The Child Pornography Prevention Act, 1996 and the Child Online Protection Act, 1998. The former Act prohibits the use of computer technology to knowingly produce child pornography, that is, depictions of sexually explicit conduct involving or appearing to involve minors. The latter Act requires commercial site operators who offer material deemed to harmful to minors to use bonafide methods to establish the identity of visitors to their site. The Communication Decency Act, 1996 has been passed to protect minors from pornography. The CDA provides any person, who knowingly transports

[27] Available at times of India. indiatimes.com@ articleshow (visited on January 26, 2019)
[28] Case of 2004 available at law mantra.co.in (visited on March 11, 2019)

obscene material for sale or distribution either in foreign or interstate commerce or through the use of an interactive computer service, shall be liable to imprisonment upto five years for a first offence and up to ten years for each subsequent offence.

In *United States v. Hilton* case[29], a federal grand jury charged Hilton for criminal possession of computer disks containing three or more images of child pornography in violation of 18 U.S.C. $ 2252A (A)(5)(B). He challenged the state without denying the charges. He contended to dismiss the charges on grounds that the Act was unconstitutional under the First Amendment. The U.S. district court was also agreed with his contention regarding the vagueness of the definition of child pornography but in this case the issue was raised whether the CPPA poses substantial problems of over breadth and which would sufficient to justify overturning the judgment of the lawmaking branches. It was held by the court that the CPPA is not unconstitutionally overbroad and the judgment of the district court is reversed.

In India, there were no laws which directly regulate cyber stalking prior February 2013 it was covered under section 66A,72 and 72 A of IT Act, 2000. In 2013, Indian parliament made amendments in Indian Penal Code, 1860 by introducing cyber stalking as criminal offence by passing Criminal Law (Amendment) Act, 2013. Cyber stalking is not directly recognized cyber crimes in India under Section 66 A by the Information Technology (Amendment) Act 2008 and under section 72, 72A. Section 66 A provides punishment for sending offensive messages through communication service etc and section 72 provides for breach of confidentiality and privacy. The Hon'able Supreme Court declared section 66 A as unconstitutional and against the freedom of speech and expression and struck it down in *Shreya Singhal and others v. Union of India*. [30]. This section had been misused by police in various states to arrest the innocent person for posting critical comments about social and political issues on networking sites. *Ritu Kohli's*[31] case was the India's first case of cyber stalking, which was registered by Economic offences Wing of Delhi Police under section 509 IPC for outraging the modesty of a woman. Section 503 0f IPC provides for stalking and also harassment. Further, section 504 provides a remedy for use of abusive and insulting language. This is another form in which cyber stalking takes place where abusive words etc. are sent through e-mail.

In United States, cyber stalking is a criminal offence under American anti-stalking, slander, and harassment laws. A conviction can result in a restraining order, probation, or criminal penalties against assailant, including jail. Cyber stalking specifically has been addressed in U.S. federal law. For example, the Violence against Women Act passed in 2000, made cyber stalking a part of the federal interstate stalking statute. Still, there remains a lack of federal legislation to specifically address cyber stalking, leaving the majority of legislative at the state level. A few states have both stalking and harassment statutes that criminalize threatening and unwanted electronic communications. The first anti-stalking law was enacted in California in 1990, and while all fifty states soon passed ant-stalking laws, by 2009 only 14 of them had laws specifically addressing "high-tech

[29] 167 F.3d 61 (1" GR.), cert. denied, 120 S. Ct. 115 (1999)
[30] AIR 2015 SC 1523
[31] Available at www.nalsarpro.org>moduls >module 4(visited on March 25, 2019)

stalking.[32]

So, in USA almost every state has laws dealing with cyber stalking. US federal Code 18 under section 2261 A (2) states that whoever with the intent uses the mail, any interactive computer service, or any facility of interstate of foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury shall be liable under section 2261 B (b) for a imprisonment which may extend upto life imprisonment if the death of the victim results; for not more than 20 years if permanent disfigurement or life threatening bodily injury to the victim results; for not more than 10 years, if serious bodily injury to the victim results or if the offender uses a dangerous weapon during the offense.

New Jersey v. Dharun Ravi, is a case of cyber stalking in which a college student named Ravi secretly made a film of his roommate's sexual intimation with another man and then posted this online. By this act of Ravi, she committed suicide and Ravi was convicted for bias intimidation and invasion of her privacy. In 2012, the judges ruled that they believe Ravi was acted out of colossal insensitivity, not hatred and sentenced him for 30 days in jail and also with fine.

The term 'cyber defamation' is not specially used and defined under section 66A of the IT Act, 2000 but it makes punishable the act of sending grossly offensive material for causing insult, annoyance or criminal intimidation in India. Indian Penal Code, 1860 deals with menace of cyber defamation under section 499 which was got extended to 'speech' and 'documents' in electronic form by the IT Act, 2000. The offence of defamation under section 499 provides for making a publishing of an imputation concerning a person such imputation have been made with intent to harm a having reason to believe that it will harm reputation of such persons. The defamatory matter is published i.e. communicated to some person other than the person about whom it is addressed. In India, an e-mail making allegations against the person to whom it is sent would not quality as a defamatory state so long as it a not sent to a third person. Statements on mailing lists and the World Wide Web world are defamatory as they would be available to persons other than the person to whom they refer. But in 2015, the Apex court declared section 66A as unconstitutional in its entirety and against the freedom of speech and expression and struck it down in *Shreya Singhal and others v. Union of India*.[33] Because misuse of Section 66-A by police in various states to arrest the innocent person for posting content deemed to be allegedly objectionable on the internet.

In USA, the Communications Decency Act (CDA), 1996 is one of the most valuable tools for protecting freedom of expression and innovation on the internet. Section 223 of the Act lays down that any person who puts the information on the web which is obscene, lewd, lascivious, filthy or indecent with intent to annoy, abuse, threaten or harass another person will be punished either with imprisonment or with fine. Section 230 of the Act provides for protection for private blocking and screening of offensive material. The section says that no provider or user of an interactive computer service shall be considered as the publisher or speaker of any information

[32] Christa Miller, "High-Tech Stalking, Law Enforcement Technology", available at: http://www.officer. com/article/10233633/high-tech-stalking (visited on March 6, 2018)

[33] AIR 2015 SC 1523

provided by any other information content provider.

In *Stratton Oakmont, Inc. v. Prodigy Services Company*[34] case, the defendant is a publisher which led to the court for holding a finding that it would be a hurdle for a plaintiff to overcome in pursuit of their claims because one who repeats or republishes a libel is subject to liability as if he had originally published it. In this case the US court clearly indicated and followed the decisions given in *cubby case* and held that it would be impossible for the provider to monitor every message posted.

In *Cubby, Inc. v. CompuServe, Inc.*[35] case, the issue was raised that whether the service provider exerted enough control over or had knowledge of or reason to know, the contents of allegedly defamatory statements posted on one of its bulletin boards. In this case the court held that the service provider was liable defamatory statements posted on its bulletin boards, notwithstanding the fact that the control it exerted over content was intended to improve its service and keep them free from objectionable material.

The term 'Phishing' is not used anywhere in India as given under IT Act, 2000 before the amendment Act, 2008. But now it is a punishable offence under section 66, 66A, 66C, 66D of IT Act, 2000 and under IPC, 1860. Section 66 A of Information Technology Act provides punishment for sending offensive messages through communication service etc. Section 66 C of Information Technology Act, 2000 which is inserted by Amendment Act, 2008 provides punishment for Identity Theft if any person whoever fraudulently or dishonestly make use of the electronic signature, password or any other unique identification features of any other person. Section 66 D is applied to any case of cheating by personating which is committed by using a computer resource or a communication device which can be used for phishing but not directly.

On January 26, 2004 the US Federal Trade Commission filed the first lawsuit against a suspected phisher. The defendant, a Californian teenager, allegedly created a webpage designed to look like the America Online website, and used it to steal credit card information[36]. After this, Senator Patrick Leahy introduced the Anti-Phishing Act in Congress on March, 2005 which would punish and fined those cyber criminals who created the fake websites and sent bogus e-mails with the purpose of defrauding consumers. But it did not pass. In Jan. 2007, Jeffrey Brett Goodin of California was become the first convicted cyber criminal by a jury under the CAN-SPAM Act, 2003 for sending thousands of e-mails to America Online users which prompted customers to submit personal credit card information. In USA, The CAN- SPAM Act, 2003 is the direct response of the growing number of complaint over spam e-mails and is also the first USA cyber law which establishes national standards

The term 'cyber fraud' is neither defined in the Indian Penal Code, 1860 nor in the IT Act, 2000. Section 66-D was inserted by the Amendment Act, 2008 for providing punishment for cheating by personation by using computer resource which is also used for cyber fraud but not directly. According to this section if any person who by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine

[34] (1995) N.Y. Misc. LEXIS 229, 1995 WL 323710 N.Y. Sup Ct. (May 24, 1995)
[35] 776 F. Supp. 135 (S.D.N.Y. 1991)
[36] Jeordan Legon, "Phishing scams reel in your identity", *CNN News*, (Jan. 26, 2004), available at: http://edition. cnn. com/2003/TECH/internet/07/21/phishing.scam/index.html?iref=newssearch (visited on March 6, 2019)

which may extend to one lakh rupees[37]. This offence is bailable, cognizable and triable by the court of Judicial Magistrate of First Class.

The USA has enacted the Computer Fraud and Abuse Act, 1996 for prohibiting and punishing computer and internet fraud which was further amended and also amended by the Patriot Act, 2001 and in 2008 by the Identity Theft Enforcement and Restitution Act. U.S Criminal Code's provisions are also applicable on the cyber fraud and the violators can be prosecuted under title 18 i.e. no. 1028 prohibits social security cards fraud and credit card frauds, no. 1029 prohibits identity fraud including telemarketing fraud, no. 1341 prohibits mail fraud, no. 1343 prohibits wire fraud etc. The Federal Statute title 18 U.S. Code s. 1030 also prohibits fraud and other related activities in connections with computers.

In *United State v. Pirello*[38] case, the defendant Pirello placed four advertisements on internet classified-ads websites for soliciting the buyers for computers with the purpose of fraudulently selling it online. By doing this, he received three orders and then he deposited the entire money received from the orders in his personal bank account but he did not delivered computers to the buyers. The court determined the issue that whether USSG 2F1.1 (b) (3), which instructs courts to enhance a sentence by two levels if the offense was committed through "mass-marketing," applied to defendants fraudulent internet advertisements. The court held that the use of the internet website to solicit orders for non-existent computers violated the USSG and affirmed the lower court's enhancement of his sentence.

Lastly, in India, Section 66 E is inserted in IT Act, 2000 after amendment in 2008 for providing punishment for violation of privacy. This section applies to the violation of the bodily privacy of any person by three stages i.e. capture, publication and transmission. This section criminalizes any of these stages that are done without the consent of the victim. It is irrelevant that whether the person to whom the mail is sent read the mail or not.

But in USA, the Electronic Communication Privacy Act, 1986 (ECPA) a criminal wiretap statute which uses the word "anyone" who commits the breach and on whom the liability can be fixed under section 2511 (1) (a). On the basis of the recommendation of the Federal Trade Corporation, the Online Privacy Protection Act, 2000 has been passed for providing protection to individual privacy.

Conclusion and Suggestions

After analysing the comparative study which is based on the legislations of both countries, it can be concluded that USA has enacted several laws for combating cyber crimes; despite this many complicated legal issues are still unresolved. In the context of India, though Information Technology Act, 2000 is a comprehensive legislation for combating cyber crimes, still it is only a gap-filler and there are so many legal issues which have no mentioned yet. The legal positions relating to electronic transactions and civil liability in cyberspace is still confused or not clear by the reason of not having any adequate laws on globally. There is a need to pass the comprehensive cyber laws globally.

In India, there has been found the number of cases of cyber crimes like cyber defamation, cyber stalking

[37] Section 66 D (Inserted Vide Information Technology (Amendment) Act, 2008)
[38] 255 F. 3d 728 (9th Cir. 2001) (USA)

and cyber harassment etc. but there is no specific definition under the Information Technology Act, 2000. It is found that a number of these types of crimes are either not registered or are registered under the existing provisions of Indian Penal Code, 1860 which are ineffective and do not cover the said cyber crimes. The Information Technology Act, 2000 has undergone with some amendments one of them is the recognition of electronic documents as evidence in a court of law. Indian Government emphasizing on encouragement to electronic fund transfers and also help in promoting electronic commerce in the country. But the result is not similar as it is. The cyber crime cells are doing training programmes for its forces and plans to organize special courses for corporate to combat cyber crime and use the Information Technology Act effectively.

There are thousands of cases taking place in the countries but only the few cases are lodged as a complaint. Because many of the victims due to the threat and fear of getting abused in the society does not move any complaint against the cyber criminals, some of the cyber victims accept this incident as nightmare or bad destiny or as wished by God and moving on the life by forgot all the incidents . But due to this the cyber criminals are more encouraged to get involved in such type of cyber criminal activities. There is need to encourage more and more complaint to be lodged for combating cyber crimes both at national and international level.

Further complicating cyber crime enforcement is the area of legal jurisdiction. No one country cannot by itself effectively enact and enforce laws that comprehensively address the problem of internet crimes without cooperation from other nations. While the major international organizations, like the OECD (Organization for Economic and Cooperation and Development) and the G-8, are seriously discussing cooperative schemes, but many countries do not share the urgency to combat cyber crimes for many reasons, including different values concerning piracy or espionage or the need to address more pressing social problems. These countries, inadvertently or not, present the cyber criminal with a safe haven to operate. [39] There is a need to decide the issue of investigation at globally.

The Information Technology Act does not have any specific provision for defining and punishing cyber spamming. In the contemporary time period spamming is the most threatening act of cyber world. Therefore, there is a need to adopt the Anti-Spam law for the protection of children. In USA, the CAN- SPAM Act, 2003 is the direct response of the growing number of complaint over spam e-mails and is also the first USA cyber law which establishes national standards for sending of commercial e-mail.

United States passed the federal laws on cyber squatting which is known as Anti-Cyber Squatting Consumer Protection Act in 1999. In India, the Information Technology Act does not have any specific provision for defining and punishing cyber squatting and these cases are decided under Trade Mark Act, 1999. Therefore, there is a need to adopt the Anti-Squatting law.

There are large number of cyber laws passed and amended in U.S.A and India. But instead of these laws the cyber crimes are increasing day by day. For example, a total of 8, 045 cases were registered under Information Technology Act during the year 2015 as compared to 7, 201 cases during the previous year 2014 and 4,356 cases

[39] Loknath Behera, "Investigating External Network Attacks", *The Indian Police Journal*, Jan.- March, 2004 at p. 27

during 2013, showing an increase of 11.7% in 2015 over 2014 and an increase of 65.3% in 2014 over 2013[40]. As compare to India, in USA for the year 2015, Cost of Data Breach Study by IBM and the Pone mom Institute revealed that the average total cost of a data breach increased from $ 3.52 million in 2014 t0 $ 3.79 million. Another study said that cyber crime will become a $ 2.1 trillion problem by 2019. [41]

In U.S.A Cyber Crime Laws are very stringent and strictly enforced. However, in India Information Technology are very loosely framed and enforcement is also lenient. USA is fully digitalized but India is not completely digitalized till now. So, in India people are not literate in Computer and also not aware about the cyber Crime. Indian police is also not fully equipped with tools and technology to combat Cyber Crimes.

[40] National Crime Records Bureau, Ministry of Home Affairs, cyber Crimes in India, at 163-164 (2015), available at: http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Compendium-15.11.16.pdf (visited on feb. 11, 2019)

[41] Limor Kissem, "2016 Cyber Crime Reloaded: Our Prediction for the Year Ahead", (Last Modified on Jan. 15, 2019), available at: https://securityintelligence.com/2016-cybercrime-reloaded-our-predictions-for-the-year-ahead