International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Cyber Crime Scenario in India and Judicial Response

Nidhi Arya

LLM, Chandigarh University, Mohali, Punjab, India

How to cite this paper: Nidhi Arya "Cyber Crime Scenario in India and Judicial Response" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.1108-1112, URL: https://www.ijtsrd.com/papers/ijtsrd24025.pdf

IJTSRD24025

ABSTRACT

The internet in India is growing rapidly. It has given rise to new opportunity in every field like – entertainment, business, sports, education etc. It is universally true that every coin has two sides, same for the internet, it uses has both advantage and disadvantage, and one of the most disadvantage is Cyber-crime.[1]

Cyber crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react[2]. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. This article is an attempt to provide a glimpse on cyber crime in India. This article is based on various reports from news media and news portal.

Keywords: *Cyber crime, Internet, Hacking, Phishing, Cyber squatting*

1. INTRODUCTION

The world of Internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines.

Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind.[1]

In present generation its rapid growth on Information Technology is enclosing all walks of life. These technical improvements have made the transformation from document to paperless communication possible. Whereas computer are meant to store privileged data of Political, social, economic which brings huge benefits to the society. The wide extension of an internet and Computer technology globally has led to escalation of internet related crimes.[2]

In recent times, India has become major spot for cyber criminals, who most hackers and other malicious users commit crimes through internet. As there as various types of cyber crimes these crimes are rising at a terrifying rate. India is ranked fifth in cyber crime amongst other countries. Under Indian law cyber crime does not have any specific definition under any Indian legislation one legislation that deals with offences related to such crime is Information technology Act, 2000 which was later amended as Information Technology Act, 2008. In order to define such an offence, it can be done through cause of action; it is a combination of computer and crime.[3]

In Asia region India has rank top two internet users country, so India is the very fastest growing country. Today internet becomes the backbone of social & economic world. Users can access the internet anytime from anywhere but through the internet many illegal works may done. Today E-mail and website is the most efficient way of data communication.[4]

2. CYBERSPACE:

The term "cyberspace " was first used by the cyberpunk science fiction author William Gibson, which he later described as an "evocative and essentially meaningless "buzzword" that could serve as a cipher for all of his cybernetic musings. Now it is used to describe anything associated with computers, information technology, the internet and the diverse internet culture. Cyberspace is the electronic medium of computer networks, in which online communication taken place and where individuals can interact, exchange ideas ,share information, provide social support, conduct business, direct actions, create artistic media, play games, engage in political discussion, and so on. It is readily identified with the interconnected information technology required to achieve the wide range of system

[1] Justice Yatindra Singh, *Cyber Laws* 36 (universal law publishing, Delhi, 6th edn.,1998)

[1] Dr. Jyoti Rattan and Dr. Vijay Rattan , *Cyber Laws & Information Technology* 47 (Bharat law publishing, Calcutta,6th edn.,2017)

[1] Dr. Faruq Ahmed, Cyber Law in India 67 (New Era Law Publication, Ahmedabad, 3rd edn., 2002)

[2] *Ibid.*

[3] B. Swaathi and M. Kannappan, "Cyber Crime-An Indian Scenario"119 *ISSN* 1053 (2018)

[4] *Ibid.*

capabilities associated with the transport of communication and control product and services.[5]

Cyberspace is the "place "where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. the place between the phones in the past twenty years, this electrical "space", which was once thin and dark and one dimensional –little more than a narrow speaking –tube, stretching from phone to phone has flung itself open like a gigantic jack-in-the-box.[6] Light has flooded upon it, the eerie light of the glowing computer screen. This dark eclectic netherworld has become a vast flowering, electronic landscape. Since the 1960s, the words of the telephone has cross-bred itself with computers and television, and though there is still no substance to cyberspace, nothing you can handle, it has a strange kind of physicality now. It makes good sense today to talk of cyberspace as a place all its own.[7]

Electricity was first harnessed in 1831, but it was not until 1882 that the first power station was built in 1882. Then it took another 50 years before reaching 80 percent in United States. Radio took 38 years to be used by 50 million people. TV took 13 years to reach 50 million people, whereas PC took 16 years to reach 50 million people. However, the internet took only 4 years to have 50 million people online; thus, increasing the horizon of cyber space.[8]

3. WHAT IS CYBER CRIME?

"Cybercrime" is a combination of two terms "crime" with the root "cyber" derived from the word "cybernetic", from the Greek, "kubernan", which means to lead or govern. The "cyber" environment includes all forms of digital activities, irrespective of whether they utilize single network. Cyberspace is borderless as no Courts across the globe can claim jurisdiction. Any illegal act which involves a computer, computer system or a computer network is cybercrime.[9]

Crime consists of engaging in conduct that has been outlawed by a society because it threatens the society's ability to maintain order.

The expression crime is defined as an act which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The offence is defined in code of criminal code of criminal procedure to make punishable by any law for the time being in force.[10]

Cyber crime is a term used to broadly describe criminal activity in which computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity.[11]

4. DEFINITION OF CYBER CRIME:

The Indian Legislature doesn't provide the exact definition of Cyber crime in any statute, even the Information Technology Act, 2000; which deals with cyber crime doesn't defined the term of cyber crime. However in general the term cybercrime means any illegal activity which is carried over or with the help of internet or computers.

In the words of **Dr. Debarati Halder** and **Dr. K. Jaishankar**, cybercrimes are "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, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)."[12]

In the words of **Pawan Duggal,** "Cyber crime refers to all the 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 activity, which basically offends human sensibilities, can be included in the ambit of cybercrimes."

In the words of **Dr. R.K. Tewari**, "cyber crime may be said those species, of which, genus in the conventional crime, and where either the computer is an object or subject of the conduct constituting crime".[13]

According to **UNO expert** recommendations, the term of "cybercrimes "covers any crime committed by using computer system or networks, within their framework or against them. Theoretically, it embraces any crime that can be committed in the electronic environment. In other words, crimes committed by using e-computers against information processed and applied in the internet can be referred to cybercrimes.[14]

In the words of **Katyal,** "cyber crimes are offences conducted in the "cyberspace" and the term "cyberspace" is ambiguous in the first place. A diverse range of act such as the spread of computer viruses, visting an obscene website and cyber stalking may qualify as a cybercrime".[15]

5. OBJECTIVES:

- To Study the implementation on enactments of cyber law.
- To know the types cyber crimes and its functions.

---

[5] Dr. Jyoti Ratan, *Cyber laws & information technology 54* (universal publication, new Delhi, 4th edn., 2014).

[6] Dr. Amita Verma , *Cyber Crimes & Law* 47(universal publication, new Delhi 1stedn., 2009)

[7] Sudershan ,Goel Ravi Sodhi, *crime law & advice* 67 (kamal public house publication, Ahmadabad, 2ndedn., 2012) .

[8] *IBID*

[9] Rohasnagpal **,** *Cyber Crime and Corporate Liability* 45 (4thedn 1997)

[10] Animesh Sarmah, Roshmi Sarmah ,Amlan Jyoti Baruah, " A brief study on Cyber Crime and Cyber Law's of India Volume: 04 Issue: 06 June 2017 (last visited on 25th October 2018)

[11] *IBID*

[12] Jonathan clough, *Principles of Cybercrime* 12(cambridge publication , 2ndedn 1998)

[13] Petter Gottschalk ,*Policing Cyber Crime* 75 (Lexix Nexix Publication , 2ndedn 2002)

[14] Deccan Chronicle , Cybercrime, *available at*: https://www.deccanchronicle.com/nation/crime/200718/indias-cybercrime-scenario-ground-situation-alarming.html (last visited on 25th October 2018)

[15] Om Bhusan , " CYBER CRIME-Definition, challenges and the cost, ISSN 2347 – 8527 Volume 3, Issue 2 April 2014" (last visited on 23rd October 2018)

- To analyze the problems faced by the police for investigation on cybercriminals.[16]

5. CYBER CRIME INCLUDES:

Following are the few examples of cyber Crime:

5.1.1. Email spoofing:

This technique is a forgery of an email header. This means that the message appears to have received from someone or somewhere other than the genuine or actual source. These tactics are usually used in spam campaigns or in phishing, because peo**p**le are probably going to open an electronic mail or an email when they think that the email has been sent by a legitimate source.[17]

5.1.2. Hacking:

Amongst all types of cyber crime it is the most dangerous and serious threat to the internet and e-commerce. Hacking refers to the secretively breaking into the computer system and stealing valuable data from the system without any permission. Spreading computer virus: It refers a set of Cyber instructions which are able to perform some malicious operations. Viruses stop the normal functioning of the system programs and insert few abnormalities. A computer viruses can be spread through- Emails, CDs, pen drives (secondary storage), Multimedia, Internet.[18]

5.1.3. Phishing:

Phishing refers to stealing information's like passwords, credit card details, usernames etc of target person/persons over the internet. Phishing is carried out by email spoofing and instant messaging. In this type of crime hackers make a direct link which directs the targeted persons to the fake page which looks and feels identical to the actual one.[19]

5.1.4. Cyber stalking:

Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

5.1.5. Cyber defamation:

Cyber defamation means the harm that is brought on the reputation of an individual in the eyes of other individual through the cyber space. The purpose of making defamatory statement is to bring down the reputation of the individual.[20]

5.1.6. Cross site scripting:

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls[21].

5.1.7. Vishing:

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the billpayer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.[22]

5.1.8. Cyber trafficking:

It may be trafficking in weapons, drugs, human beings, which affect the large numbers of persons.

5.1.9. Web jacking:

The term Web jacking has been derived from hi jacking. In this offence the attacker creates a fake website and when the victim opens the link a new page appears with the message and they need to click another link. If the victim clicks the link that looks real he will redirected to a fake page. These types of attacks are done to get entrance or to get access and controls the site of another. The attacker may also change the information of the victim's webpage.[23]

5.1.10. Malicious Software:

These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

5.1.11. SMS Spoofing:

SMS Spoofing allows changing the name or number text messages appear to come from.[24]

6. ROLE OF JUDICIARY IN EXPANDING CYBER CRIME JURISPRUDENCE:

A. The Bank NSP Case:

In this case a management trainee of a bank got engaged to a marriage. The couple used to exchange many emails using the company's computers. After some time they had broken

---

[16] R. P. Kataria & S. K. P. Sriniwas, *Cyber Crimes* 22 (Orient Publishing Company, New Delhi 1stedn 2016)

[17] Classification of cyber law, *available at*:https://www.scribd.com/doc/316141735/Characteristics-of-Cyber-Crime (last visited on 2ndnov. 2018)

[18] *Ibid.*

[19] Cyber Crime mans safety , *available at:* http://www.sbsnagarpolice.com/Cyber_crime.htm (last visited on 12 October 2018)

[20] *Ibid.*

[21] Hemraj Saini, Yerra Shankar Rao, T. C. Panda, "Cyber-Crimes and their Impacts: A Review" IJERA, Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209, (last visited 23rd October 2018)

[22] Raghav Punj ,Cybercrime ,*available at*: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (last visited on 18th October 2018)

[23] *Ibid.*

1) [24] Computer Crime, *available at*: https://www.lectlaw.com/mjl/cl025.htm (last visited on 22nd October 2018)

up their marriage and the young lady created some fake email ids such as "Indian bar associations" and sent mails to the boy's foreign clients. She used the banks computer to do this. The boy's company lost a huge number of clients and took the bank to court. The bank was held liable for the emails sent using the bank's system.[25]

B. Bazee.com case:

In December 2004 the Chief Executive Officer of Bazee.com was arrested because he was selling a compact disk (CD) with offensive material on the website, and even CD was also conjointly sold-out in the market of Delhi. The Delhi police and therefore the Mumbai Police got into action and later the CEO was free on bail.[26]

C. Parliament Attack Case:

The Bureau of Police Research and Development, Hyderabad had handled this case. A laptop was recovered from the terrorist who attacked the Parliament. The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir. However careful detection proved that it was all forged and made on the laptop.[27]

D. Andhra Pradesh Tax Case:

The owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 was recovered from his house by the Vigilance Department. They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were conducted. It had been concealed that the suspect was running 5 businesses beneath the presence of 1 company and used fake and computerized vouchers to show sales records and save tax. So the dubious techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.[28]

E. State of Tamil Nadu v. Suhas Katti,[29] decided by a Chennai court in 2004. The woman, a divorcee, complained to the police about a man who was sending her obscene, defamatory and annoying messages in a Yahoo message group, after she turned down his proposal for a marriage. The accused opened a fake email account in the name of the woman, and forwarded emails received in that account. The victim also received phone calls by people who believed that she was soliciting for sex work .The police complaint was lodged in February 2004 and within a short span of seven months from the filing of the First Information Report, the Chennai Cyber Crime Cell achieved a conviction. Katti was punished with two years' rigorous imprisonment and Rs. 500 fine under S. 469 IPC (forgery for the purpose of harming reputation), one year's simple imprisonment and Rs. 500 for offence under S. 509 IPC (words, gestures or acts intended to insult the modesty of a woman) and two years' rigorous imprisonment and Rs. 4000 fine for offence under S. 67 of IT Act 2000 (punishment for publishing or transmitting obscene material in electronic form).[30]

F. Fatima Riswana v. State Represented by ACP, Chennai and other,[31] both the public prosecutor and counsel for the petitioners applied to the court for transfer to another (male) judge, to save the district lady judge from embarrassment of having to view certain CDs that are part of the evidence. The order for transfer was passed and the justification for this was that the "said trial would be about the exploitation of women and their use in sexual escapades by the accused, and the evidence in the case is in the form of CDs. and viewing of which would be necessary in the course of the trial, therefore, for a woman Presiding Officer it would cause embarrassment."[32]

G. S.M.C. Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra[33] India's first case of cyber defamation case, In this case, the defendant Jogesh Kwatra being an employ of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff. On behalf of the plaintiffs it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature.[34]

H. Air force Bal Bharti School Case[35] was filed in the Juvenile court, Delhi on the charge of cyber pornography. Some jurists say this is the first Indian cyber pornographic case which was charge sheeted in the juvenile court. The brief facts in issue were that a student of the Air force Bal Bharti School, Lodhi Road, New Delhi was arrested by the Delhi Police in the year 2001 April.

[25] State by Cyber Crime Police vs. Abubakar Siddique

[26] Avnish Bajaj vs. State (N.C.T.) Of Delhi 3 Comp LJ 364 Del, 116 (2005) DLT 427, 2005 (79) DRJ 576

[27] State vs. Mohammad Afjal Delhi 1, 107 (2003) DLT 385, 2003 (71) DRJ 178, 2003 (3) JCC 1669

[28] Andhra Pradesh State Road vs. The Income-Tax Officer 1964 AIR SCR (7) 17.

[29] Decided by the Chief Metropolitan Magistrate, Egmore, on November 5, 2004

[30] Order passed on 5 November 2004 in CC No. 4680 of 2004 by the Chief Metropolitan Magistrates Court, Egmore, Chennai (India

[31] Criminal Appeal 63 of 2005 arising out of SLP (Cri) No. 1606 of 2004 decided by the Supreme Court on January 11, 2005

[32] Dr. M. Sanjeeva Rao, " Pornography Needs Strict Regulations in India" Volume 1 *ISSN* 211(2016)

[33] Smc Pneumatics (India) Pvt. Ltd vs Shri Jogesh Kwatra on 12 February, 2014

[34] Case List: Cyber Defamation, available at: https://indiancaselaws.wordpress.com/2014/08/23/case-list-cyber-defamation/ last visited: march 7 2019)

[35] The Air Force bal Bharti, Delhi Cyber Pornography Case 2001

The alleged accused was then a class XII student who created a pornographic website as revenge of being teased by classmates and teachers. He listed in that website the name of his 12 school mates 'girls and teachers in sexually explicit manner. He was then suspended by the School Authorities though the juvenile court allowed his bail prayer. However, he was charged under s. 67 of the Information Technology Act 2000, and ss. 292, 293, 294 of the Indian Penal Code and the Indecent Representation of Women Act. The most significant steps were taken by the law enforcement agencies in India.

Further, Honble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world as also in cyberspace which is derogatory or defamatory or abusive of the plaintiff.[36]

I. Shreya Singhal v. U.O.I[37] this is a landmark judgment, concerning section 66A of the Information Technology Act, 2000. This Section was not in the Act as originally enacted, but came into force by virtue of an Amendment Act of 2009 with effect from 27.10.2009.[38]

The reason behind the insertion of section 66A according to the Amendment Bill was:
"A rapid increase in the use of computer and internet has given rise to new forms of crimes like publishing sexually explicit materials in electronic form, video voyeurism, and breach of confidentiality and leakage of data by intermediary, e-commerce frauds like personation commonly known as Phishing, identity theft and offensive messages through communication services. So, penal provisions are required to be included in the Information Technology Act, the Indian Penal code, the Indian Evidence Act and the Code of Criminal Procedure to prevent such crimes".[39]

Facts:
The Petitioners have raised a large number of points as to the constitutionality of section 66A. According to them, first and foremost Section 66A infringes the fundamental right to freedom of speech and expression and is not saved by any of the eight subjects covered in Article 19(2).[40]

Further, in creating an offence, section 66A suffers from the vice of vagueness because unlike the offence created by section 66 of the same Act, none of the aforesaid terms are even attempted to be defined and cannot be defined, the result being that innocent persons are also roped in. Such persons are not told clearly on which side of the line they fall; and it would be open to the authorities to be as arbitrary and whimsical as they like in booking such persons under the said section. In fact, a large number of innocent persons have been booked.[41]

The Court held that the provision of section 66A of the IT Act is derogative to the Article 19(1) (a) and as such it is an arbitrary provision which breaches the right of citizen to have freedom of speech and expression of their views on internet. As such the provision concerned is constitutionally invalid and as such struck down in its entirety.[42]

7. CONCLUSION

It is cleared from the previous studies and records that with the increment in technology cybercrimes increases. Qualified people commit crime more so, there is need to know about principles and computer ethics for their use in proper manner. Cybercrime and hacking is not going away, if anything it is getting stronger. By studying past incidents, we can learn from them and use that information to prevent future crime. Cyber law will need to change and evolve as quickly as hackers do if it has any hopes of controlling cybercrime. Law must also find a balance between protecting citizens from crime, and infringing on their rights. The great thing about the internet is how vast and free it is. Will it be able to remain the same way while becoming tougher on criminals? Only time will tell. There will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists but we can win only through partnership and collaboration of both individuals and government. There is much we can do to ensure a safe, secure and trustworthy computing environment. It is crucial not only to our national sense of well-being, but also to our national security and economy. Yet India has taken a lot of steps to stop cybercrime but the cyber law cannot afford to be static, it has to change with the changing time.

[36] Debarti Halder, *Child Sexual Abuse and Protection Laws in India* (Universal Law Publishing, 1st edn.,2018)
[37] Shreya Singhal v. Union of India [AIR 2015 SC 1523]
[38] *Ibid.*
[39] Akash dhanjani, "Case Brief Shreya Singhal v/s Union of India, 2015" available at: https://lawbriefs.in/case-brief-shreya-singhal-v-s-union-of-india-2015/ last visited on: March 4. 2019
[40] Information Technology Act 2000, India, available at: http://www.mit.gov.in/itbill.asp (last visited on March 7, 2019
[41] *Ibid.*
[42] Suhrith Parthasarathy "The judgment that silenced Section 66A" *The Hindu,* March 8, 2019.