CYBERCRIME IN INDIA

Himanshu Morwal, Manipal University Jaipur

ABSTRACT

The era of technological revolution has served the interest of people all around the globe. There has been a dynamic explosion in the technological development since the inception of Internet nearly two decades ago. Internet is considered an integral part of human life. This technological advancement has eased up the life of the people in various aspects. It has also caused menace to the society in the form of Internet crimes which are committed online, with the use of any computer or network, also known as Cybercrime. With the rapid increase in internet users, it has also given rise to several online crimes such as cyber stalking, cyber pornography, spoofing, phishing, cyberbullying etc. These crimes have made people vulnerable and skeptical. The paper aims to instill a brief understanding of the concept of cybercrimes, various methods of cybercrimes frequently used, and also to identify the root cause of cybercrimes, applicability of legal provisions, and effective preventive measures against such crimes. This paper aims at recognizing the sheer need to ratify the legal frame work for stringent punishment against the cybercriminals but also providing legal remedies to the victim and ensuring a congenial and secured environment for them to access internet.

Keywords: Internet, Cybercrime, Cybercriminals, Information Technology Act, IPC

Introduction

Since the emergence of civilization, the humankind has been constantly thriving for progress, invention and technologies for survival and out of all remarkable discoveries and advances made by the mankind, invention of computer is a noteworthy achievement which has bought ease to the human life and also helped in storing the human knowledge in a more feasible manner for future usage. The technological revolution prospered with the new dimension called Internet. The proliferation of information available on the internet has offered a massive scope, opportunities and served the interest of the society as a whole. This proliferation and diffusion of information is unequivocally considered to be boon for the humankind but has also allowed transgression of various forms and crimes committed online, which is also knows as Cybercrime. Since these crimes are committed online it is difficult to ascertain the geographical location, boundaries, distances etc. therefore, the cyber criminals remains undetectable. And conclusively, it has grave repercussions of ineffable magnitude.

Computers do not commit crimes. Cybercrime are the offences which are commissioned online through the use of computer. It consists of various illegal activities which could cause immense harm to an individual, society and to the state with the criminal mind which intends to cause mental or physical harm or injury or harm to the reputation of the victim either directly or indirectly through the use of Internet. Technology plays a crucial role in commissioning cybercrimes and most of the perpetrators are technically skilled who are well versed and thorough with the internet and the applications. In recent times, the women have majorly became the muse for cyber criminals and they are explicitly exploited and bullied over the course of time due to their vulnerability and lack of experience, knowledge about the vices of the internet, they are more susceptible and becomes the bait for the criminals and bullies online. Due to the veil of anonymity on the internet, this gives the cyber criminals an edge to exploit, harass, bully young girls, lone working women and these criminals many a times lure them into sharing their bank account details, personal photographs etc. and thus women becomes the soft target and an easy prey for these criminals than men. Cybercrimes such as cyber stalking, cyber spoofing, phishing, spoofing, cyber bullying, cyber pornography etc. have been significantly rising high in the last two decades which has raised concern because it is still considered a grey area which requires a more unified definite law and the Information Technology Act 2000 was enacted to boost e-commerce, e-trading business but have not been efficient in dealing with cybercrimes.

Cyber Law deals with the Information exchange across the Internet through any computer system. With the advent of various novel modes of communication systems, it has transformed our life styles by making it easier, but has created a digital space where we are more prone towards crimes. Majorly all companies extensively sustain upon their computer networks retaining their data in electronic form, consumers are using master cards, credit-debit cards for shopping. Almost everyone uses e-mails, Cell phone, SMS messages, social media and other online platforms to communicate in day-to-day routine. Big organizations, Industries are extensively dependent upon computers to create podcast and arrange all data safe in the electronic devices rather than traditional paper documents as they are easily accessible and easier to locate. Features like Digital signatures and e-contracts are fast replacing conventional method of transacting business.

History of Internet in India

The internet is the vast computer network that stores and carries information around the world. Internet was initially available in India through ERNET. It was made available for commercial purpose by the Videsh Sanchar Nigam Limited (VSNL) in August 1995.It is significant to mention that theinitial phenomenon of data hacking from the Bhabha Atomic Research Centre (BARC) transpired in 1998, which is considered first proclaimed case of Cybercrime in India. With an aim to defy computer and Internet related crimes, a new legislation was enacted by the Indian Parliament, the Information Technology Act, 2000, which may be said to be a milestone in India's Internet journey to tackle the problems created by the development of information technology.

On October 17, 2000, the Information Technology Act came into force. The Act deals with various provisions of Internet related crimes precisely in context with virus attacks, unauthorized access, , denial of assess or any pervasion causing willful abrasion to computer software etc. However, there still exis tcertain grey areas that exist in the cyber law mainly because Information Technology Act is primarily meant to be a legislation to promote e-commerce and therefore, it has not proved very efficient in dealing with newly emerging cybercrimes. An expert committee was appointed in 2005 to suggest amendments for the shortcomings in this act. It was on the recommendation of this Committee that the Information Technology (Amendment) Bill 2006 was introduced in the Parliament on December 15,2006 and finally passed by both the Houses on December 24, 2008.

The Information Technology (Amendment) Act, 2008 (Act 10 of 2009) received Presidential assent on February 5, 2009. Rules have also been framed under the amended Act which became effective from October 27, 2009.

Concept of "Cybercrime"

Those infringements which emanates on or using the instrument of the Internet are known as Cybercrimes. Cybercrime has been defined by ***Oxford Online*** "as a crime committed online".

Cybercrime is defined as "Any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime". (Hinduja, 2007)

In another words, "Cybercrime may be said to be those species of a genus which is the conventional crime and where either the computer is an object or subject of the conduct constituting crime"[1]. (Pandey,2006)

The cybercrimes are committed with the advent usage of Technology and therefore, the delinquent of these crimes are mostly high-tech professionals who have vastinsight of the internet world and the functioning of computer applications. To name a few Cybercrimes such as cyber-stalking, cyber- terrorism, e-mail spoofing, e-mail, bombing, cyber pornography, cyber defamation, polymorphic virus, worms etc. are widely acknowledged by Cyber experts due to repetitive reports of these crimes with Cyber Cell across the globe. Few accustomed crimes can be counted cybercrimes when any act takes place through middling of Internet viz. cheating, fraud, misrepresentation, theft, pornography, intimidation, threats etc. All these crimes are penalized under the Indian Penal Code, 1860.

There is no statutory or legal definition of Cybercrime defined anywhere. A simple yet tenacious definition of Internet-related crime is stated as, "unlawful acts wherein the computer is either a too or a target or both" (Nagpal, 2008). Thus cybercrimes are the crimes directed at a computer or a computer system or a computer network.

Reasons for growth in Cybercrimes

Professor H.L.A. Hart in his outstanding work entitled "The concept of Law" has stated that mankind is susceptible and vulnerable to unlawful acts which are crimes and therefore, requires

[1] *"Cybercrime in India* by Prof. Kavita Singh, Blog on -*India Criminal Law*. Reference given in Pandey, *Ashish, "CYBERCRIMINAL DETETION AND PREVENTION", JBA PUBLISHER, DELHI, 2006*

profound set of rule of law to protect them against such acts (Hart, 2012). Applicability of similar analogy to cyber space, the computer systems despite being technologically advanced systems, is utterly vulnerable. As there is no bullet proof mechanism present to protect and safeguard innocent users from hackers and their criminal activities. People who tend to commit cybercrimes becomes fearless as in many instances the criminal activity becomes untraceable due to erasing of records and data along with the use of VPN (Virtual Private Network) which can be used to fool the trackers and destroy own virtual identity.

The reasons for vulnerability of computer systems to cyber criminality are stated as follows:

1. **Huge Data Capacity:**

Computers in this modern Era have a tendency to store a large amount of data for almost eternal time. A small microprocessor computer chip can store lacks of pages, images, videos for a very minimal cost which are very easy to access and transfer.

2. **Wider Access to Information:**

Prodigious benefit of networking in the era of computer is the wider access to data availability on massive scale. Large number of organizations is resorting to web of networks for providing easily accessible data to their, customers and parties and even to employers. Information promulgation through Internet has channeled new pathways for rapidity and cost effective methods for simple access to information across the globe.

3. **Negligence of Internet Users:**

Carelessness often lands a person in deep trouble and sometimes proves to be a costly affair. Similarly, if no proper steps are taken for safeguarding computer system, this might give opportunity to cyber attackers togain unethical access to computer system..

4. **Inadequacy or Loss of Evidence:**

Preservation of evidence in Cyber world gives a hard time to investigating agencies and Cyber Police. Unlike the usual crimes, it is burdensome to gather adequate corroborated facts and data of a cybercrime which can establish the offence committed by the cybercriminals beyond suspicion because internet being widest medium, makes it difficult to trace the origination of crime. Thus, due to lack of penalized provisions against cybercriminals, it acts like a shield to these criminals who destroy the evidences to escape from getting convicted.

Techniques of Committing Cybercrimes:

1. **Hacking/ Unethical access to Computer system:**

When an unknown person gains access of a computer system without permission to fulfill devious purpose is commonly called Hacking. For a better understanding, the term hacking is interchangeably used and perceived as 'unauthorized access'. Hacking can be done for the sake of challenge or as an adventure, in order to do unlawful activity or because of the habit. Hacking can be done by way of two types i.e. against computer and against network. Hacking in simple words means unlawful penetration into someone else's computer in order to steal data, photographs, files, documents etc. with ill intention of causing harm and injury to a person reputation or goodwill.

2. Stealing Information contained in Electronic Form:

Any information stored in computer hard disks, removable storage media, hidden folders etc. the stored information can be easily stolen, either by retrieving the data physically or by tampering them through the virtual medium.

3. E-Mail Bombing:

It is a mischievous act where a large amount of e-mails are sent to victim's e-mail account resulting in server. Like any other cybercrime it is committed for causing trouble to victim and is difficult to ascertain the origin and location of sender. Such acts are done in an attempt to overflow the victim's inbox or to lower the frequency of server to carry out fraudulent activities..

4.Data Diddling:

This mode of crime is considered the easiest cybercrime involving a nunauthorized attack on computer by altering raw data either by a person or through programmed. This cybercrime is committed to disrupt the network activities carried on a particular device or system.

5. **Salami Attack**:

This mode of crime is agile and substantially takes place in the financial establishments or enterprises for the purpose of monetary-based crimes. Essential characteristic of such offence is that the modification is so petty that it is generally overlooked.

6. Cybercrimes against privacy:

In cybercrimes involving violation of right to privacy, the computer system is used as a tool for perpetrating the criminal act. Truly speaking, several behaviors stated above as cybercrimes of economic type are similar to those that would correspond to this category of cybercrime, the only difference being that the behavior would not affect any proprietary right of the victim, instead would affect his legal right such asright to privacy.

7. **Stalking:**

In general sense stalking can be defined as an act or conduct in which the victim is followed or stalked virtually either through some social media account or random websites with the motive of harassing traumatizing, terrorized, frightened, intimidating etc. . In cyber stalking, the internet is used to pursue, harass or contact another in unsolicited fashion. A lot of stalkers resort to stalk a victim or target offline- in order to gain dominance over them. On the Contrary,in physically following or stalking,the stalker may physically harm or inflict serious injuries like acid attack or attacking with some sharp objects. In Internet stalking, the stalker pursue the victim virtually and has no fear of physical avenge since its impossible to get caught in cyberspace. Cyber stalking is often interchangeably used with the term "cyber teasing".

In the case of **Ritu Kohli (**Ahmad, 2008**),**It is regarded as the first reported case of Cybercrime in India, where the victim became the target of a cybercriminal who used her identity to chat on a social media account. Later it was also found that the criminal has also distributed her number to other person and she was receiving calls at odd time and it all created havoc in her personal life. The criminal was later arrested by tracing the Internet Protocol (IP) address and the case was reported under section509 of Indian Penal Code, 1860.

Some other cybercrimes to which criminals often resort to-

(a) Spoofing :-

Spoofing or E-mail spoofing is a cybercrime which is used to commit cyber financial frauds. In this kind of cybercrime, the identity of the victim/target can be easily personified and there is also very less risk of being caught**.**

(b) Spamming :-

Spamming or Spam Junk is another type of cybercrime in which the criminals lure the investors into a virtual scheme and policy and solicit money after gaining access of the investor account. This type of cyber fraud can be committed against a large number of investors at the same time by also mass-e-mailing of unsolicited messages.

(c) **Phishing :-**

Phishing is regarded as the most common and most dangerous of all kinds of e-mail fraud. This type of cybercrime is committed by well-polished technically skill-crafted criminals, who deceive victim/target through message or pop-up message shining on the monitor when they visit some website and then they send message such as "Validate", "Update" in relation to security update, bank account details, confidential data and any such information which could hamper and harm the victim if disclosed, and put him under the gun, wanting and threatening the victim to click on the icon and then re-directed to the linked page which looks legitimate but is a web waiting for the prey to fell into it. In **Sukanto v. State of West Bengal**[2] case which is relating to a magazine 'Nara Nari' for publication of obscene material, section 292 of IPC convicted the petitioner for giving effect to public morality above art, literature.

Other Two well-known illustrative cases of pornography are:-

In**Air Force Bal Bharti School**[3], a boy was pestered by classmates for having a cratered face. Fed up with evil jokes, he decided to avenge at his mockers and set up a website with pornographic material uploaded morphed indecent photographs of his class fellows and school teacherson free web-hosting service. The situation unfolded when father of one of the class-girls featured on the website and official complaint was registered with Delhi Police. The counsel representing the girl's parents who had filed the complaint said that there would be no compromise on the issue and the boy accused of setting up the website with pornographic material must be rusticated from the school. He claimed that there were other twelve children of the school whose names were mentioned in the website and the parents of these children wanted the expulsion of the accused from the school as they did not want their children to study with him.

In **Bombay Swiss Couple Case**,[4] Swiss couple assembled a flock of slum- dwellers children and madethem pose in abominable photographs. Those images were sharedexplicitly for pedophiles on adult content webpages. Police took cognizance of the complaint filed against the Swiss-Couple for pornography and they were held liablefor the shrewd offence under

[2]AIR 1952 Cal 214
[3]The Air Force Bal Bharti,(2001) Delhi Cyber Pornography Case
[4]Swiss couple cyber pornography case (2003), Mumbai

section 67 under Information Technology Act, 2000,to be read with Section 292 of Indian Penal Code, 1860.

Punishments and Penalties

THE INFORMATION TECHNOLOGY ACT, 2000

The rising incidence of cybercrimes due to fast development of computer technology necessitated enactment of separate law for prevention and control of electronic communication, the Parliament enacted the Information Technology Act, 2000 as a regulatory measure with the objective to tackle cyber offences and also to provide legal recognition to future of new-aged mode of communication by substituting the traditional mode of communication i.e. paper for storage of large amount of information, to initiate online services in various government portals for easy accessibility and mobility for citizens of the country and promote various means of electronic communications..

This Act is based on the "UNCITRAL" Model Law on E-Commerce from 1996, which was adopted in response to a United Nations General Assembly resolution urging member states to follow the UNCITRAL (United Nations Commissions on International Trade Law).Enact or revise their laws to create a uniform environment for regulating e-commerce at the international level. In view of this objective, the Act also incorporates provisions for prevention and control of offences which are the result of e-commerce and e-governance. It is one and only Act in India which deals which is called as Cyber Law of India.This act was enacted with the idea of enhancing dimensions of virtual communication via concept of digitalization and definedpunishment and penalties for cybercriminals and whoever violates certain provisions and guidelines. The relevant provisions are contained in Chapter IX and chapter XI of the Act.

Penalties for Cybercrimes

Section 65 – Tempering of Computer Source Document

Section 66 - Computer related offences.

Section 67 - Punishment for publishing or transmitting obscene material in electronic form

Section 72 -Penalty for breach of confidentiality

Section 76 - Confiscation

Section 77 –Compensation, penalties or confiscation not to interfere with other punishment: The above section states that no award of compensation, penalty levied, or confiscation rendered under this Act will prohibit the award of compensation or enforcement of any other penalty or punishment under any other statute.

Section 78 - Power to investigate offences: This provision of IT act states that no officer below the rank of Inspector shall investigate such non-cognizable offence which falls within the limits and shall be investigated by same powers as mentioned under section 156 of Code of Civil Procedure, 1973.

Punishment under IPC[5]

With the evolution of modern-era, there has been considerable change in the criminal behavior and pattern and this gave birth to the concept of cybercrime. IPC is regarded as the universal criminal law of India. The Indian Penal Code is the complete manual which covers the wide range of offences of any kind. Even though, cybercrime is the creation of new-aged technology committed through the use of computer or any other electronic device, IPC has efficiently covered the cyber related offences under the Code like the rest of the conventional crime. Because of the universal approach the conventional statutory criminal law is sufficient in dealing with cybercrime and any other crime. Some of the provisions are stated below-

Section 354 (d): Stalking

Section 383: Extortion/Web Jacking

Section 420: Cheating and dishonestly inducing delivery of property**.**

Section 464: Making a false Document

Section 468: Forgery of electronic records

Section 503: Sending threat messages by email

Section 500: Email Abuse

Section 503: Criminal Intimidation

[5]Indian Penal Code (1860)

Section 506: Punishment for Criminal Intimation

Section 507: Criminal Intimidation by Unidentified Networks or Communication

Section 509: Word, gesture or act intended to insult the modesty of a woman.

Information Technology (Amendment) Act, 2008

Due to emergence of various cybercrimes which does not fall within the ambit of Information Technology Act and to fill in the technical loopholes in the IT Act 2000, the amendment act was enacted. This act was implemented with the purpose to overcome difficulties and widen the scope of the act which not only covers the various illegal cybercrimes and illicit activities but also expanding scope of cyber laws, controlling authority and stringent punishment and provisions. The act included definitions under section 2(ha) defining Communication device and in Section 2(w) included service provider.

As Section 66 of IT Act consist of various cyber related offences, the amendment act insertion important provisions such as-

Sec 66 (A): punishment for sending of offensive messages; Sec 66(B): receiving stolen computer; Sec 66 (C): Punishment for Identity theft;Sec 66 (D): Punishment for cheating by personation by using computer resource;Sec 66 (E): Punishment for violation of privacy; Sec 66 (F): Punishment for Cyber terrorism. The punishment under sec 66 has also enhanced denoting a positive approach. In Hacking, the punishment has been increased to three years with fine from two lakhs to five lakhs. While the punishment in sec 66(F) is life imprisonment. Under sec 67, the term of punishment has been reduced to three years and fine is increased to five lakhs (ten lakhs for subsequent conviction). Insertion of sec 67 (A) has been of utmost importance from the viewpoint of curbing menace of MMS and video voyeurism with conviction for a period of five years and fine up to ten lakhs.The term of punishment and fine is also enhanced to term up to five years and fine up to five lakhs or both under Sec 72.

Preventive Measure of Cybercrime

Regardless of the penal provisions and preventive measures embedded in the Indian Penal Code and the Information Technology Act, an analysis of past year's Cybercrime statistics shows that the crime rate has not significantly reduced but, in contrast, has been growing exponentially.

Many emerging cybercrimes are surfacing, necessitating improvised forensic and legal strategies and expertise in order to effectively deal with them(Paranjape, 2009). Some essential preventive tips:-

- One must avoid disclosing any information pertaining to oneself
- One must avoid sending any photograph online particularly to strangers and chat friends.
- Never upload your credit card information to a website that's not protected.
- It is important to keep an eye on the websites that your children access in order to prevent harassment and other forms of violence.
- To defend from virus attacks, do use the most current and modified antivirus tools.

Conclusion

The prodigious growth of Internet usage in India laterally accompanied by substantial whirling of cybercrimes in India and has made the country vulnerable and susceptible to cybercriminals. The umpteen rise in no of internet users is at verge of being duped and exploited in various new forms of cybercrimes which needs to be addressed.As the cybercrimes are committed globally it becomes very difficult to nab the offenders within geographic boundaries. And it gives the offenders massive opportunities and confidence to become invincible and fearless. And, at times when cybercrimes are committed on foreign land, it takes longer than usual because of different laws in countries. Consequently, justice is delayed and victim continues to suffer and be exploited.In such cases, the cyber cells needs to appoint ethical hackers which could help the units in reaching out in shortest time span. There is dire need for Information Technology Act, 2000 to define terms like cybercrime, fraud etc. which falls off from the ambit of the Act. The proliferation in registration of various cybercrimes under IT Act and IPC clearly indicates the severity of the situation and the rise in cybercrimes constantly poses a huge threat for a country like India due to its poor infrastructure. Therefore,equilibrium has to be maintained between advanced technology and infrastructure along with social awareness and enforcement of strong cyber security lawsfor safe and protected access to the internet is the need of the hour.

REFERENCES

1. Pandey, A. (2006)*Cybercrime Detention & Prevention*, JBA Publication (1st Ed)Karol Bagh, New Delhi
2. Parker, Donn B. (1997)"Automated Crime in Cyber Crime", International Conference Course Book
3. Paranjape. V.N, (2009), "*Criminology and Penology*" Central Law Publications (14th Ed)(208)
4. Ahmad, F, (2008)"Cyber Law of India" *Law on Internet*, New Era Law Publication, (3rd Ed)(411).
5. Nagpal, R. (2008)"What is Cybercrime?"*Evolutions of Cybercrimes*, Asian School of Cyber laws
6. Hinduja S.(2007) "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