CYBER CRIMES

Shreya Jetly, Amity Law School, Noida

ABSTARCT

There has been advancement in technology, the uses of internet have been exceeded over the years which results in risks like crimes. Crimes relating to the use of internet are known as Cyber Crime which are very dangerous as compared to rest of the crimes in the world. In India, cyber laws are contained in the Information Technology Act, 2000 which was later amended in the year 2008. The paper contains the definition, evolution, history and various modes of cybercrimes like email spoofing, cyber defamations, Trojans, spamming, phishing, data-diddling etc and under which category they fall. This paper talks about the law of cybercrime in India. This paper tries to track down the concept of cybercrimes in detail and its law in India. The type of research applied here is Doctrinal. This research focuses on case-law, statutes, and other legal sources. This paper is based on exploratory research from internet and data cited in the paper, library books etc. There are primary sources like Legislation: Information Technology Act 2000 and the 2008 amended act of information and technology etc as well as secondary sources like articles and other sources like internet are being used in this research paper.

Introduction

Computer's invention has made human life very easy as computers are used for various purposes by individuals and by large organizations across the globe. "Computer is defined as a machine that stores and processes information."[1] There are erroneous purposes of computers for personal or other benefits since years. The arrival of the computer is a benefit to students, lawyers, businessmen, teachers, doctors, researchers and not to forget the criminals.

The term Internet is defined as the collection of voluminous computers that gives a network of electronic connections between the computers. These days all computers connected to the internet. These days computers and internet became very necessary and useful for our daily life. With the arrival of new technologies and the advancement in the mode of communications, the Internet has become a new form of life. It is one of the fastest modes of communication and has spread its arms, covering all possible shades of mankind. Everything has its Pros and Cons the same is with the computers.

Due to the use of computers and internet, cyber-attacks / cyber hacking has become common, which has given rise to Cybercrimes.

"Cybercrime combines the term crime with the root cyber from the word cybernetic, from the Greek, kubernân, which means to lead or govern, and Cybercrimes are committed using computers or computer networks like internet."[2]

The "cyber" environment involves all kinds of digital activities, no matter whether they are conducted through networks. This extends the previous term "computer crime" to embrace crimes committed by exploiting the Internet, all digital crimes, and crimes involving telecommunications networks. This terminology is more recent as it covers a wide variety of facets, dealing with emerging issues that also reflect its diversity.

"Crime is a social and economic phenomenon and is as old as the human society."[3]

---

[1] What is a computer, available at: https://studyres.com/doc/10035097/what-is-a-computer%3F (last visited on January, 2021).

[2] Yougal Joshi, Anand Singh, "A Study on Cyber Crime and Security Scenario in INDIA" in International Journal of Engineering and Management Research, Volume-3 https://www.termpaperwarehouse.com/essay-on/Cybercrimes/464629

[3] Vinay Kumar Gupta, "Cyber Crimes against Individuals in India and IT Act", Scribd, Page No.1.

Crime is a legal concept which has the sanction of the law. Crime is a legal wrong that leads to criminal proceedings which may further result into punishment.

"The hallmark of criminality is that it is breach of the criminal law and as per Lord Atkin the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences and a crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequence."[4]

Cybercrimes are criminal activities that are related to the use of computers, for illegally trespassing into the computer system or of another etc.

Cybercrime is the most dangerous crimes as compared to other types of crimes.

Cybercrime causes a huge amount of the loss which is evident from the number of cases coming before the criminal justice system and at the same time it is very easy to commit this crime by maintaining anonymity.

Definition of Cyber Crime:

"According to United Nations Definition of Cybercrime - At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined as:

i. Cybercrime in a narrow sense (computer crime) is any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed with them.

ii. Cybercrime in a broader sense (computer-related crime) is any illegal behaviour committed by in relation to a computer system or network, including such crimes as illegal possession offering or distributing the information by the means of a computer system or network"[5] .

Cyber Crime is also in simple words defined as the offences or crimes that takes place over electronic communications. These types of crimes are illegal activities which involve a computer and a network. Due to development of the internet, there is voluminous increase in cybercrime

[4] Ramesh Bajiya, "Conventional Crime", Scribd, Page No.1.
[5] United Nations Definition of Cybercrime, available at https://idn-wi.com/united-nations-definition-cybercrime/ (last visit May27,2020)

activities because when committing a crime there is no longer a need for the physical present of the criminal.

Cybercrimes can be also defined as "Crimes directed at a computer or computer system" But the complex nature of cybercrimes cannot be sufficiently expressed in such simple and limited term"[6]. "The Organization for Economic Co-operation and Development (OECD) recommended the working definition of cybercrime computer related crime is considered as any illegal, unethical or unauthorized behaviour relating to the automatic processing and the transmission of data"[7].

Indian legal system has enacted the Information Technology Act 2000, but it does not provide any definition of cybercrime. In Indian legal system only, this act is known as a cyber law.

Other definitions of cybercrime are:

1. A criminal activity that involves unlawful access to or utilization of computer system.
2. Any illegal action in which a computer is use as a tool or object of a crime; in other words, any crime, the means, or purpose of which is to influence the functions of a computer.
3. Any violation of the law in which computer is a target of or the means for committing crime.
4. Any activity, which involves the unauthorized and unlawful access to or utilization of computer system or network to tamper with the help of computers and the internet, can broadly be called as cybercrime.

Essentials of Cybercrime:

The term cybercrime cannot define due to its critical nature as it involves the crime relating to computer and computer techniques.

Cybercrimes are easy to commit, difficult to detect and even harder to prove due to these crimes have been characterize as low risk high rewarding ventures for the cyber criminals who cause great damage to the victims of crimes with having only basic knowledge and skill of using the computers.

[6] Cybercrime: Talat Fatima, (2011) Eastern Book Company, Lucknow. Page 89.
[7] The Criminal Aspect in Cyber Law in The Indian Cyber Law, Suresh T. Vishwanathan, (2001) Bharat Law House, Jaipur Page 7.

Many a times even the victim affected by cybercrime is unaware of its occurrence because of lack of adequate skill and lack of knowing how in handle the computer system. Cybercrime can be committed even from a far distant place without the necessity of its perpetrator's physical presence at the scene of crime and partly because detection of these crimes requires hi-tech skill which the investigators generally lack. This is truer in the case of crimes like cyber pornography, cyber defamation deceit etc. The reluctance to file a complaint worsens the significance of the problems of cybercrime detection and control.

Another feature of the cybercrime is that it becomes more difficult to detect when perpetrators thereof is an insider who is an employee working in the organization, company or the enterprise.

Cybercrimes have been characterized as high-tech offences as they are committed by the abuse of computer networks and telecommunication technology.

The range of such crime is wide enough to affect the socio-economic and the legal rights of the people. Through, the use of computer network system is legal but the illegal actions in using the networks as a medium are deemed illegal and punishable under the criminal law or the cyber law or even under both the laws. Like any other crime the hi-tech cybercrime committed through the computer telecommunication networks has the following:

i. The perpetrators as well as the victim both remain anonymous and difficult to be identified.
ii. Several unspecified potential customers are used through they will be far away from the place of crime.
iii. Evidence against the crime is easy to erase thus rendering the victim helpless.

The consequences of cybercrimes are widely spreading. Certain cybercrime affects the personal record of the individual, which violate the right to privacy, in some cases it may get the personal code of the banking account and may cause huge financial loss. If the banking and financial sectors affect, it may also upset marketing equilibrium or break down the same by denial of service.

History of Cyber Crime

"In the year 1820 first cybercrime was recorded. The primeval type of computer has been in Japan, China, and India since 3500 B.C, but Charles Babbage's analytical engine is considered as the time of present-day computers. In the year 1820, in France a textile manufacturer named Joseph-

Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened and prefer to sabotage to discourage Jacquard so that the new technology cannot be utilized in the future"[8].

Modes / Classifications of Cyber Crime

Cyber Crime can be classified into four major categories as follows: -

i. Cyber Crime against individuals
ii. Cyber Crime against property
iii. Cyber Crime against organization
iv. Cyber Crime against society

i. Cyber Crime against individuals: Crimes that are committed by the cyber criminals against an individual or a person, some of them are -

a) Email spoofing: This technique is a forgery of an email header. In this the message is received from a non-genuine source.

b) Spamming: Email spam which is otherwise called as junk email. It is undesired message sent through email. The uses of this type of cybercrime become popular in the mid-1990s and it is a problem faced by most email users till now. Spam Bots obtain the recipient's email id and spam bots are automated programs which crawls over the internet in email id search. Spam Bots are used by the spammers to create email distribution. As the responds to a spam mail is quite low so the spammer sends an email to millions of email addresses.

[8] History of Cyber Crime in short - International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 06 | June -2017 - A brief study on Cyber Crime and Cyber Law's of India

c) 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 and the purpose of making defamatory statement is to bring down the reputation of the individual"[9].

d) IRC Crime (Internet Relay Chat): IRC servers allow the people around the world to come together under a single platform which is sometime called as rooms and they chat to each other. Cyber Criminals basically uses it for meeting. Hacker uses it for discussing their techniques. It is used to allure small children by the paedophiles.

e) Phishing: In this type of crimes or fraud the attackers tries to gain information such as login information or account's information by masquerading as a reputable individual or entity in various communication channels or in email.

There are many other cybercrimes against individuals includes- Net extortion, Credit Card, Malicious code etc.

ii. Cyber Crime against property: These types of crimes include vandalism of computers, Intellectual (Copyright, patented, trademark etc) Property Crimes, online threatening etc. Intellectual property crime includes:

a) Software piracy: It can be described as the copying of software by unauthorized way.

b) Copyright infringement: It can be described as the infringements of an individual or organization's copyright. In simple term it can also be describes as the using of copyright materials such as music, software, text etc in an unauthorized manner.

c) Trademark infringement: It can be described as the using of a service mark or trademark in an unauthorized way.

iii. Cyber Crime against organization: Cyber Crimes against organization are as follows:

a) Unauthorized changing or deleting of data.

[9]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 @ IJTSRD | Unique Paper ID - IJTSRD24025 | Volume – 3 | Issue – 4 | May-Jun 2019 Page: 1108 Cyber Crime Scenario in India and Judicial Response Nidhi Arya

b) Reading or copying of confidential information in an unauthorized manner, but the data are neither being change nor deleted.

c) DOS attack: In this attack, the attacker floods the servers, systems, or networks with traffic to overwhelm the victim resources and make it difficult for the users to use them.

d) Email bombing: In this massive numbers of emails are sent to an email address to flood the mailbox with mails, and it is a sort of Net Abuse.

e) Salami attack: The other name of Salami attack is Salami slicing. To seize the customer's information like bank details, credit card details etc the attackers use an online database.

f) Attacker deduces very little amounts from every account over a period. In this attack there is no complaint is filed and the hackers remain free from detection as the clients are unaware of the slicing.

g) Data Diddling – In this attack the raw data is altered before it is processed by the computer and then then after the process is complete the changes are back. For example: When Electricity board was being computerised, it faced data diddling.

h) Logical bomb – this is event dependent program which means when the event triggers or occurs these programs are created to do something.

i) Torjan horse – A Trojan is an unauthorized program which functions from inside by falsely representing to be an authorized program, thereby concealing what it is doing.

iv. **Cyber Crime against society**: Cyber Crime against society includes:

a. Forgery: Forgery means making of false document, signature, currency, revenue stamp etc.

b. Web jacking: The term is derived from the word hi jacking. In this kind of 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 and if the victim clicks the link that looks real to him, he will be redirected to a fake page. To get the access and controls and to change the site's information these attacks are done on the victim's webpage.

Cyber Criminals

The classification of cyber criminals is based on the object that they have in their mind while committing such crimes.

1. **Children and adolescents between the age group of 6 – 18 years** because of their tendency to know and explore various things and sometimes to prove their unique qualities, children can become cyber criminals. Though it is hard to believe that kids can also be cyber criminals whether knowingly or unknowingly. The most amateur hackers comprise of teenagers. It happens to be a matter of pride for the teenagers to be able to hack into a computer system or to a website. Children may commit the crimes without knowing that what they are doing is a crime.
2. **Organised hackers –** they have their own targets to achieve, Hackers who come together with a particular motive are called hacktivists. These groups operate on a political basis.
3. **Professional hackers or crackers –** they are employed to hack the site of the rivals reliable and valuable information. Due to extensive computerization business organizations storage of information in electronic form in. These are employed by rival organizations to steal other industrial information and secrets which can prove to be beneficial for them.
4. **Discontented employees** – these people include those who have been either sacked by their employer or are dissatisfied with their employer. To take revenge they use these kinds of criminal activities. Disgruntled employers can do a lot more harm to their employers by committing crimes via computers which can bring their entire system down with the increase in dependence on computers and automation of processes.

Cyber Law

Cyber law deals with legal issues concerning the internet, cyberspace. Cyber law controls the crimes committed through the internet or through the uses of the computer resources. It prevents the users by reducing large scale damage from cybercriminal activities by protecting information, intellectual property, piracy, and the freedom of speech related to the use of the websites, emails, cell phones, computers, software, and hardware, such as data storage devices.

Cyber law plays a very important role in this modern era of technology. With the increased dependence of e-commerce and e-governance a wide range of legal issues related to use of internet as well as other forms of computer or digital processing devices for instance violation of intellectual property, piracy, freedom of expression, etc. that has emerged and needs to be tackled through the instrumentality of law.

Cyber laws inter alia cover a few topics of the Indian penal Code[10] , Intellectual Property Rights, The Indian Evidence Act[11], Companies Act[12] and others but still it does not hold enough to cover the huge scope of cyber-crimes.

Several new crimes related to computers and internets have evolved in the society due to vast increase in the use of Internet. Such crimes where use of computers used with Internet are termed as **Cyber Crimes.**

Cyber related Laws revolves mainly around:

a. Cyber crimes

b. Electronic and digital signatures

c. Intellectual property

d. Data protection

As the tendency of misusing of technology is rising day by day, there is a need of strict statutory laws to regulate such criminal activities in the cyber world with a true purpose of protecting technology **"Information Technology Act, 2000"[13][ITA- 2000]** enacted by Indian Parliament to protect the fields of e-commerce, e-governance, e-banking as well as punishments in the field of cybercrimes and was further amended as **"IT Amendment Act, 2008 [ITAA-2008], it increased** the scope and applicability of ITA-2000**"**[14]**.**

IT Act Amendment of 2008 added Section 66A which deals with publishing of threatening, offensive, or false information and was later criticized for being in violation of Article 19 of the Indian Constitution[15] concerning freedom of speech and expression. The exceptions to this Article are on grounds of Defamation, incitement to crime, contempt of court public order decency morality friendly relations with neighbours, national security.

The freedom of speech and expression through electronic means i.e. over internet and other e-sources are restricted under Section 66A and in no case it is included even in the restrictions

[10] he Indian Penal Code, 1860 (Act 45 of 1860)
[11] The Indian Evidence Act, 1872 (Act 1of 1872)
[12] The Companies Act, 2013 (Act 18 of 2013)
[13] Information Technology Act, 2000, available at https://www.advocatekhoj.com/library/bareacts/informationtechnology/index.php?Title=Information%20Technology%20Act,%202000 (last visit May3,2020)
[14] Information Technology (Amendment) Act, 2008, available at https://www.bcasonline.org/Referencer2015-16/Other%20Laws/information_technology_act_000.html (last visit May3,2020)
[15] The Constitution of India,1949, Art.19.

provided in Article 19 of the Indian Constitution. For instance, it punishes one for sending messages which cause annoyance or hurt the sentiments or knowing it to be wrong. Many petitions were filed which challenged the constitutionality of S.66. In one of the leading case of SHREYA SINGHAL V. UNION OF INDIA[16], the Supreme Court examined the Indian, English and US law on free discourse, struck down Section 66A of the Information Technology Act as it was over-expansive and ambiguous and violated Article 19(2) of the Constitution

The Section 66A (E-mail related offences), Section 66F (punishment for cyber terrorism i.e. imprisonment for life), Section 67B (exacting arrangement for Child Pornography), Section 66B (maintenance of stolen PC gadgets) have included an alternate view in the field of the digital wrongdoing. Sections 67, 67A alongside Section 66 permits security against profanity.

"Information Protection" is given importance under Section 43A and Section 72A. Section 43 is currently connected with Section 66 and for the offences where there is disallowed access, and which is hurtful to the PC framework and to the clients.

Section 67C is a prevailing area that builds the duties of organizations and middle people and furthermore adds extraordinary forces to Section 65. Sections 69,69A and 69B bolstered by Section 70B give tremendous forces to Government organizations to permit data security in the Cyber Space which incorporates families and private corporate division.

Forces to control data security in the Government frameworks is given under Section 70. Sections 71, 73 and 74 give insurance to the Digital Signature framework.66C and 66 D deal with the identity misuse which are done in the way of password theft or other sources.

Conclusion

In present world people are more and more dependent upon cyber technology due to which cybercrime are rapidly increase. The advancement of the human civilized society has facilitated by digital technology. An issue of cybercrime is just not in the minds of law makers, but also concerns the administrators, government, and local users. “Changes are inevitable and the dilemmas that advancement in technology cannot be avoided, the truth is that the criminals have changed their method and have started relying at advanced technology and in order to deal with them the society the legal and law enforcement authorities, the private corporations and

[16] AIR 2015 SC 1523.

organizations will also have to change." Such experts should not solely be knowledgeable however should even be given necessary technical hardware and software so that they can efficiently fight the cyber criminals. Thus, various necessary facilities must be established so that crime in the virtual world can be contained. Another aspect is that a culture of continuous education and learning needs to be introduced together with the legal and the law enforcement authorities because the IT field is a dynamic field as the knowledge of today becomes obsolete in a short time. Protection of cybercrimes in India is given in the other legislations like IT ACT (the information and technology act) which came into force in 2000 and later it was amended in 2008, which provides that the act was passed with the objective to give legal recognition for transactions carried out by means of electronic data and other e-commerce means.

The act has made amendments to various other legislations like the Indian Penal Code 1860, Indian Evidence Act 1872, the Bankers Books of Evidence Act 1891, and the Reserve Bank of India Act 1934 for easement of legal recognition and regulation commercial activities. The objective is not to suppress the criminal activity; this act has defined certain offences and penalties to smother such omissions, which is to be understood within the characterization of cybercrimes. It is inferred that the law cannot afford to be static, it needs change with the changing times. The governing laws of cyber technology contains each and every aspect and issues relating to cybercrime and further grow in continuous and healthy manner to keep constant vigilant check over the related crimes.

Thus, with the rapidly changing technology our laws are also slowly changing and are trying to be up to date.