International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue-01
January 2018

Cyber Crimes in India

Dr Rinku
Assistant Prof in law, C.R. Institute of Law, Rohtak.

The term 'cybercrime' is a misnomer. This term has nowhere been defined in any Act passed or enacted by the Indian Parliament. The concept of cybercrime is not radically different from the concept of conventional crime. Both include conduct whether act or omission, which cause breach of rules of law and counterbalanced by the sanction of the state[1].

Before discussing the concept of cybercrime it is necessary to differentiate between Conventional crimes and cybercrime.

Crime or an offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment[2]." The hallmark of criminality is that, it is breach of the criminal law. 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. On the other hand Cybercrime is the latest and perhaps the most complicated problem in the cyber world. "Cybercrime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime" "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cybercrime[3]"

Cybercrime may be defined as unlawful acts wherein the computer is either a tool or target or both. The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

According to WIKIPEDIA ENCYCLOPEDIA, a Cyber-crime consists

[1] Cyber crime by Parthasarathi Pati available at www.naavi.org visited on 28th August 2017 at 5:00 P.M.
[2] Ibid.
[3] Ibid.

of all criminal offences which are committed with the aid of communication devices in a network. This can be for example the internet, the telephone line or the mobile network.

The advent of computer has been a boon to students, lawyers, businessmen, doctors, teachers and criminals. Unauthorised access and damage to property, theft and the distribution of obscene and indecent material are all familiar crimes and have assumed new dimensions with the emergence of the internet. The internet is fast becoming a way of life for millions of people; however it is also being transformed into a haven for criminals.

There have been various kinds of computer and internet related crimes. The most common amongst these is the use of viruses to corrupt or to destroy data stored in computer systems. Other forms of fraud, robbery and forgery also exist. Bogus schemes on the internet have already robbed many people of a vast amount of money. In fact, the growth of crime on the internet is directly proportional to the growth of the internet itself and so is the variety of crimes being committed or attempted.

The Budapest Treaty of November, 2001 is the first ever Convention on cybercrime. It is first treaty on criminal offence against, with or with the help of computer networks or internet[4]. There are various kind of cybercrime. They are[5]-

I. Digital Forgery

Forgery is a creation of a document which one knows is not genuine and yet projects the same as if it is genuine. In common parlance, it is used more in terms of affixing somebody else's signature on a document. Digital forgery implies making use of digital technology to forge a document.

Section 91 of the IT Act amended the provisions of the IPC in relation to forgery to include electronic records as well. Section 29A has been inserted in the Indian Penal Code to provide for a definition of electronic record. The words electronic record will have the same meaning which is assigned to it in clause (t) of sub-section (1) of section 2 of the IT Act.

Therefore, Digital forgery and offences related to it are now covered under the IPC pursuant to the amendments made by the IT Act.

II. Cyber Pornography

[4] Nandan kamath-law relating to computers ,internet and e-commerce at p-208

[5]Pavan Duggal, " Cyber Law – An Exhaustive Section Wise Commentary On The Information Technology Act Along With Rules, Regulations, Policies, Notifications Etc" at p.5

Cyber pornography refers to stimulating sexual or other erotic activity over the internet. This would include pornographic websites, pornographic magazines produced using computers to publish and print the material and the internet to download and transmit pornographic pictures, photos, photos, writings etc[6]. In recent times, there have been innumerable instances of promotion of pornography through the use of computers. Information technology has made it much easier to create and distribute pornographic materials through the internet. Such materials can be transmitted all over the world in a matter of seconds.

The issue of cyber pornography has been dealt with in section 67 of the IT Act where publishing of information which is obscene in electronic form has been made an offence. The section provides that whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees[7].

Other enactments having a bearing on the issue are Indecent Representation of Women's Act, 1986 and Young Persons (Harmful Publication) Act, 1950.

III. Alteration and Destruction of Digital Information

The single largest menace facing the world of computers, today, is the threat of corruption and destruction of digital information induced by a human agent with the help of various types of programmes. The most commonly known programmes can be classified broadly into the following categories:

- Virus
- Trojan Horse
- Worms and
- Logic Bombs

A computer virus is a programme designed to replicate and spread, generally with the victim being oblivious to its existence.

[6] http://cybercrimecentre.in visited on 24th Oct.2017 at 7:00 P.M

[7] The Information Technology Act, 2000

Computer viruses spread by attaching themselves to other programmes or to the boot sector of the disk. When an infected file is activated or executed or when the computer is started from an infected disk, the virus itself is also executed[8].

Trojan Horse is a malicious, security breaking program that is disguised as something benign such as a directory lister, archive, game or even a programme to find and destroy viruses.

A Worm is program that propagates itself over a network, reproducing itself as it goes. Therefore, worm unlike a virus, does not require a medium to propagate itself and infect others.

A Logic Bomb is a code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security compromising activity whenever specified conditions are met.

Section 43(c) of the IT Act covers the area of introduction of viruses etc. It provides that if any person without permission of the owner or person in charge introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. The explanation to the section further defines 'computer contaminant' and 'computer virus'. Computer contaminant means any set of computer instructions that are designed (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network or (b) by any means to usurp the normal operation of the computer, computer system or computer network.

Computer virus means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource or operation when a programme, data or instruction is executed or some other event takes place in that computer resource.

IV. Hacking / Unauthorised Access

There are various kinds of hackers. The word "hacker" is used to describe all of these.

1. Code Hackers-They know computers inside out. They can make the computer do nearly anything they want it to.

[8]Barkha, " Cyber Law and Crimes", online available on www.legalserviceindia.com visited on 11th Sept 2017.

2. Crackers-They break into computer systems. Circumventing Operating Systems and their security is their favourite pastime.

3. Cyber Punks-They are the masters of cryptography.

4.Phreakers-They combine their in-depth knowledge of the Internet and the mass telecommunications systems.

Hackers are becoming a menace so uncontrollable that even the largest companies in the world are finding it difficult to cope up with their incessant attacks. Some hackers "enjoy" cracking systems and gaining access to them, they do not intend to commit any further crime.

V. Cyber Stalking / Harassment[9]

Cyber stalking, which is simply an extension of the physical term of stalking, is used to refer to the use of the internet, e-mail or other electronic communication device to stalk another person. Stalking generally involves harassing or threatening behaviour 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 or vandalizing a person's property.

Though cyber stalking does not involve any physical contact, yet, stalking through the internet has found favour among the offenders for certain advantages available like, ease of communication, access to personal information and anonymity.

Offline and online cyber stalking have certain differences, which make the latter more dangerous. In specific, in online cyberstalking, the cyberstalker can be geographically located anywhere. In few instances, the cyberstalker does not even directly harass his victim. Rather, he would post such comments on a common discussion board that would prompt the other users to send messages to the victim under a misconceived notion.

VI. Fraud on the Internet[10]

Internet fraud is a form of white-collar crime whose growth may be as rapid and diverse as the growth of the Internet itself.The types of Internet fraud schemes that law enforcement authorities are identifying extend well beyond securities-based transactions to many other situations, such as spurious investment and business opportunities, online auctions, sales of computer and Internet related

[9] http://www.helplinelaw.com/family-law/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html visited on 27th Sept 2017.

[10] Ibid.

products and services, and credit card issuing. In fact, the diversity of areas in which the Internet is being used to defraud people and organisations is astounding. There are various types of fraud-

• On line Investment Newsletters: Hundreds of online investment newsletters have appeared on the Internet in recent years. Many ¬offer investors seemingly unbiased information free of charge about featured companies or recommending "stock picks of the month". While legitimate online newsletters can help investors gather valuable information, some online newsletters are tools for fraud.

• Bulletin Boards: Online bulletin boards-whether newsgroups , usenet, or web-based-have become an increasingly popular forum for investors to share information. Bulletin boards typically feature "threads" made up of numerous messages on various investment opportunities.

• Email Online Spams: Because "spam"-junk email-is so cheap and easy to create, fraudsters increasingly use it to find investors for bogus investment schemes or to spread false information about a company. Spam allows the unscrupulous to target many potential investors. Using a bulk email programme, spammers can send personalised messages to thousands and even millions of Internet users at a time.

These offences can be related, most conveniently, to the offences of fraud and cheating.

VII. Defamation on the Internet[11]

Another grey area is with regard to law of defamation and the internet. There are a plethora of issues related to internet defamation. These include questions of jurisdiction and also questions relating to lack of legal awareness amongst people using the Internet.

The most important issue relates to the question of whether writings on the Internet amount to "publication" or not. To consider this question, it is essential to examine the distinct sites where defamation may occur on the internet. These are:

• One-to-one e-mail messages: E-mail is a remarkably quick and easy to use method of correspondence. It has closer resemblance to spoken conversation rather than written interaction. Psychologically, electronic interaction combines a sort of deceptive distance with a kind of equally deceptive intimacy. There is a tendency to make inappropriate statements. Hence, email

[11] http://cybercellmumbai.gov.in/ visited on 26th jan 2017.

senders are dangerously prone to making defamatory statements.

• Mailing lists: The format of an electronic mailing list is that various parties subscribe by email to it. A central host administers it. In a mailing list, the user sends mail to every member of the list. This increases the possibilities of being liable for defamation.

• Newsgroups: These are discussion fora that are made up of comments from their subscribers and sorted out by subject matter. Hence, any comment posted to a Usenet news group is virtually guaranteed to be published and read within days in hundreds of countries across the world. Newsgroups are the most problematic from the point of view of defamation.

• World Wide Web: The World Wide Web is the largest growing component of the Internet. It combines a user-friendly interface with freedom of articulation and information. This results in people who have no knowledge of the law of defamation writing defamatory statements without appreciating their potential liability.

VIII. BREACH OF CONFIDENTIALITY AND PRIVACY[12]

The meaning of the words 'confidentiality' and 'privacy' are somewhat synonymous. Confidentiality involves a sense of 'expressed' or 'implied' contractual obligation. It may also exist independently of any contract, on the basis of an independent equitable principle of confidence. Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others. In the legal parlance, the issue of confidentiality comes up where an obligation of confidence arises between a 'data collector' and a 'data subject'. This may flow from a variety of circumstances or in relation to different types of information, which could be employment, medical or financial information. An obligation of confidence gives the data subject the right not to have his information used for other purposes or disclosed without his permission unless there are other overriding reasons in the public interest for this to happen. That is, where an obligation of confidence arises, it is unlawful for a data user to use the information for a purpose other than that for which it was provided. Hence, "right" is an interest recognized and protected by moral or legal rules. It is an interest, the violation of which would be a legal wrong. Respect for such interest would be a legal duty. It is the basic principle of

[12] Ibid.

jurisprudence that every right has a correlative duty and every duty has a correlative right. But the rule is not absolute. It is subject to certain exceptions in the sense that a person may have a right but there may not be a correlative duty. Nevertheless, it would prudent if the issues related to privacy (and confidentiality) are viewed as 'right along with duties'.

Law of privacy in India-

Though the Constitution of India has not guaranteed the right to privacy; fundamental right to the citizens but nevertheless, the Supreme Court has come to the rescue of common citizen, time and again by construing "right to privacy" as a part of the right to" protection of life and personal liberty".

Even the fundamental right "to freedom of speech and expression" enumerated in Article 19(1)(a)[13] comes with reasonable restrictions imposed by State relating to (i) defamation; (ii) contempt of court; (iii) decency or moral (iv) security of the State; (v) friendly relations with foreign states; (vi) incitement to an offence; (vii) public order; (viii) maintenance of the sovereignty and integrity of India. Thus, the right to privacy is limited against defamation, decency or morality.

Moreover, the right to privacy could also be read into Article 21 which states that "no person shall be deprived of his life or personal liberty except accord to procedures established by law". In the context of personal liberty, the Supreme Court has observed that "those who feel called upon to deprive other person their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law".

Sale of illegal articles[14]

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or 167 simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

Online gambling

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

Intellectual Property crimes

[13] The Indian Constitution.

[14] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

Email spoofing[15]

A spoofed email is one that appears to originate from one source but actually has been sent from another source. E.g. Rahul has an e-mail address rahul@asianlaws.org. His enemy, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Rahul, his friends could take offence and relationships could be spoiled for life. Email spoofing can also cause monetary damage loss.

In short we can say that with the advancement of technology the criminals have find out new means for committing crimes in cyber space. It is difficult to punish the cybercriminal due to lack of jurisdiction and it is also difficult to trace such offenders. Here the world has to come together to prevent these offences.

[15] "Cybercrime— what are the costs to victims - North Denver News". North Denver News. Retrieved 16 May 2015.