DE JURE NEXUS LAW JOURNAL

Author:

Jai Giridhar

Symbiosis Law School, Noida

1st Year, BBA LL.B.

CYBER CRIME AGAINST INDIVIDUAL, ORGANIZATION AND GOVERNMENT

ABSTRACT:

Humans have become increasingly dependent on the internet for all of their needs as technology improves. We can now get instant access to everything while sitting in one place thanks to the internet. Every conceivable activity, including social networking, online shopping, data storage, gaming, online schooling, and online jobs, may be accomplished over the internet. The internet is used in almost every facet of daily life. The concept of cybercrime rose in popularity as the internet and its attendant benefits expanded in popularity. With the growing reliance on the internet, new sorts of cybercrime have emerged.

KEYWORDS:

Cybercrime, information technology, digital, stalking, internet, spamming, digital privacy.

INTRODUCTION

To build the understanding about cyber crime first we need to understand what is cyber. Cyber is a word that denotes Information technology (IT), it talks about things related to computing and various other things which falls under this category like-internet etc. It talks about the relationship between modern technology and computing and early computing like in 1980's and 90's is not generally termed as cyber.

Cyber crime is also known as computer crime, it includes usage of a computer in such a manner or as an instrument for illegal activities, some of the examples of cybercrime are- committing fraud, stealing identities, interference with the privacy of others. In the early times most of the victims and doers of cybercrime were Americans, as they adopted the usage of computers and internet earlier than other countries.

DEFINING CYBERCRIME

The development of new technologies brings new criminal opportunities and thus leads to new types of crime, now let us understand difference between cybercrime and traditional criminal activity: -

Digital computing- It is one of the major differences, but it is not the only difference between cybercrime and realms of criminal activity. To violate someone's privacy, commit fraud, steal someone's identity it is not necessary to be done by computer or any digital support. Cybercrime is a prefix, it especially involves internet, a digital and electronic source. It can be the attack on information about individuals, corporations, governments etc.. This attack is not on the physical body rather on the virtual body of people or corporate in today's world our virtual identities are important to us and play an important role in our day-to-day life.

In network as well in real world internet offers criminals with multiple hiding places. But just like other criminals despite their best efforts, cyber criminals also leave some clues behind them, skilled trackers can follow these clues and catch them.

Cyber Crime Against Individual

As we know that cybercrime is an unlawful act as the name itself says and is done with the hep of computer wherein the computer can be used as the tool or target or both.

The computer can be used as a tool in activities like- financial crimes, child pornography, sale of illegal articles, cyber stalking, forgery and many more.

Activities where computer can be the target- unauthorized access to computer, e-mail bombing, web jacking, theft of information contained in the electronic forms, physical damage to the computer system.

There is a distinct type of cybercrime which is 'Cyber Harassment'. There are many types to harassment that occur in cyberspace or may occur by using it. It can be in the form of religious, racial, sexual harassment or any other. It can also be violation of privacy of citizens.

Some of the ways which can be used as the weapons against a person in cyber space: -

E-mail Spamming-

Some of the names of this are Email spam, junk email, unsolicited bulk email (UCB). Same message is sent to a person many times that it forces the person to gain attention on the message sent by them.

E-mail Bombing-

It occurs through sending threatening E-mails. For example- Mr. X sent an E-mail to Mr. A and called him to be 'his friend'. That E-mail contained some private information of Mr. A's company and in the same E-mail Mr. X said that to keep this information secret Mr. A have to give Rs. 10000 every month to him. If don't do so his information will be leaked.

IRC Related Crime-

The three most common ways of IRC attack are flood attacks, verbal attacks and clone attacks.

a) Flood attack: Flood attacks cause users with slower computers to freeze up because the attacker sends a large number of random characters to the server. When an attacker combines two or more of these techniques, the result is a worst-case scenario.

b) Clone attacks: Clone attacks occur when hundreds of individuals connect to the same IRC server via a socks proxy or Trojan virus, overloading the server or forcing clients with slower machines to freeze up.

c) Verbal attack: It refers to verbally abusing people on server.

Cyber stalking-

It means to stalk someone with the help of internet or any electronic device, which can result into a computer crime or harassment. Some of its other names are online harassment or online

abuse. Here the stalker does not harm the person physically but gathers information through electronic device and internet to make threats or any verbal intimidation.

Some other weapons are Cyber Pornography, Phishing, Cyber smearing.

How To File a Complaint

The complaints can be made to in-charge of cyber cells, to file a complaint following documents are required:

1. In case of hacking:

a) Server logs

b) Copy of defaced web page in soft copy as well as hard copy format, if your website is defaced

c) If data is compromised on your server or computer or any other network equipment, soft copy of original

d) Data and soft copy of compromised data.

e) Access control mechanism details i.e.- who had what kind of the access to the compromised system

f) List of suspects – if the victim is having any suspicion on anyone.

g) All relevant information leading to the answers to following questions –

h) What? (What is compromised)

i) Who? (Who might have compromised system)

j) When? (When the system was compromised)

k) Why? (Why the system might have been compromised)

l) Where? (Where is the impact of attack-identifying the target system from the network)

m) How many? (How many systems have been compromised by the attack.

In case of vulgar E-mail:

a) Bring hard as well as soft copy of the offending e-mail.

b) Do not delete that e-mail.

c) Save the copy of that e-mail on the hard drive of the computer.

CYBERCRIME AGAINST ORGANIZATION:

Cybercrime against organization mainly includes, web jacking, industrial spying, unauthorized access to computer, denial to service attack, forgery, crimes emanating from internet group, malware attack, network intrusions, password sniffing etc.

CYBERCRIME AGAINST GOVERNMENT:

This is the least prevalent type of cybercrime, yet it is also the most serious. Cyber terrorism is a crime committed against the government. Hacking government and military websites, as well as delivering propaganda, are examples of government cybercrime. Terrorists or foreign countries' enemies are frequently the perpetrators of these crimes.

With the help of internet there are certain offences done by certain groups, with the intent to threaten the governments. It includes:

Cyber terrorism:

It is one of the most major issues in the global as well as in the domestic concern. Terrorist assaults on the Internet commonly take the shape of distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks, and so on. Cyber terrorism puts the nation's sovereignty and integrity in jeopardy.

Cyber Warfare:

It is the politically motivated hacking for the purpose of damage and spying. It is a type of information warfare that is sometimes compared to conventional warfare, albeit this comparison is debatable in terms of truth and political intent.

Distribution of pirated software:

It is the distribution of pirated software from one computer system to the another with the intention to destroy the data and records of the government.

Possession of unauthorized software:

With the help of internet, it is very easy to access any information by terrorists and to possess it for social, political, ideological, religious objectives.

JUDICIAL INTERPRETATIONS:

1)Shankar v. State Rep

Facts: The petitioner filed a motion to suppress the charge sheet filed against him under Section 482, CrPC. The petitioner was accused under Sections 66, 70, and 72 of the IT Act for gaining unauthorised access to the protected system of the Legal Advisor of the Directorate of Vigilance and Anti-Corruption (DVAC).

Decision: The charge sheet submitted against the petitioner cannot be annulled under the statute of non-granting of sanction of prosecution under Section 72 of the IT Act, according to the Court.

2)State of Tamil Nadu v. Suhas Katti:

The current case represents a watershed moment in the Cyber Law regime because of the speed with which it was handled, resulting in a conviction within seven months of the FIR being filed.

Facts: The accused was the victim's family friend who intended to marry her, but she married another man, resulting in a divorce. After her divorce, the accused persuaded her once more, and in response to her refusal to marry him, he utilised the Internet to harass her. The accused created a fake e-mail account in the victim's name and used it to send defamatory, vulgar, and harassing messages to the victim.

A charge sheet was filed against the accused person under Section 67 of the IT Act and Section 467 and 509 of the Indian Penal Code (IPC), 1860.

Decision: The accused was found guilty under Sections 469 and 509 of the Indian Penal Code, 1860, and Section 67 of the Information Technology Act by the Additional Chief Metropolitan Magistrate at Egmore. The accused was sentenced to two years in prison and a fine of Rs. 500 under Section 469 of the Indian Penal Code, one year in prison and a fine of Rs. 500 under Section 509 of the IPC, and two years in prison and a fine of Rs. 4,000 under Section 67 of the Information Technology Act.

CONCLUSION:

Cyber Crimes are of various types like Cyber-crime against Individual, Government, Organization, under them they are of various kinds. One must be careful and conscious about it. One must read the cookies, terms and conditions before accepting it on any website, always

keep the antiviruses on the computers updated in order to stay protected from any cybercrime. If face any cybercrime must complaint about it, by following the steps mentioned above.