CYBER CRIME AND CYBER LAWS OF INDIA

By Muskaan Sharma,

Student BA LL. B Asian Law College

ABSTRACT

As we have a tendency to all understand that this can be the age wherever most of the items square measure done sometimes over the web beginning from on-line dealing to the net dealings. Since the online is considered as worldwide stage, anyone will access the resources of the web from anyplace. The web technology has been exploitation by the few individuals for criminal activities like unauthorized access to other's network, scams etc. These criminal activities or the offense/crime associated with the internet is termed as cyber crime. So as to prevent or to punish the cyber criminals the term "Cyber Law" was introduced. We will outline cyber law because it is that the a part of the legal systems that deals with the web, cyberspace, and with the legal problems. It covers a broad space, encompassing many subtopics in addition as freedom of expressions, access to and utilization of the web, and on-line security or on-line privacy. Generically, it's alluded because the law of the online.

Key Words: Internet, Unauthorized access, Cyber Crime, Cyber law ,punish, Network

INTRODUCTION

We reside in associate degree era wherever the web has become a vicinity of our daily schedule. Everything, from ordering food to look online, learning an issue to viewing memes, posting online regarding your whereabouts to online transactions, has been therefore graven in our functioning that we tend to overlook the threats, and dangers it poses to North American nation. The net could be a worldwide stage, which implies that anyone will have access to that. And once individuals have access to something, they begin violating it.

Computer fraud can be a untrustworthy misrepresentation of the fact proposed to prompt another to abstain from doing something that causes loss. Computer crime can be summarized as a criminal activity which involves information technology infrastructure, in addition to unauthorized access,

illegal interception, any data interference, computer or systems interference, abusage of devices, forgery, blackmail, embezzlement, and some electronic fraud. There exits privacy issues whenever any confidential information or data is hijack or lost, either lawfully or otherwise.

Cyber crime cells are there in states basically to handle these crimes, and to expel or punish the netizens or criminals committing any of the cyber crime . It basically ranges from theft of an individual's identity entire disruption of a particular country's Internet and network connectivity due to massive attacks across its networking resources. In this digital age, online communication now become a norm, the internet users and the government are at a enlarged risk of becoming the bull's-eye of the cyber attacks. Cyber crime can cause harm to any organization. Hacking of the ATM password, transferring the money by hacking the bank account details of the victim's account to theirs, some pornography issues etc , are some of the thefts that are handled by educated people .There is an urge to implement some of the rules and regulations, to tackle and handle these crimes governing cyber space particularly known as Cyber Law.

Cyber security requires global co-operation to deal with the security of cyber space [3]. It protects computer equipment's, resources of computer or system, information and data from any unauthorized access and the disclosure .During this paper different kinds of attacks and threats are overviewed. Each and every attack is described firmly, category of hackers are also reviewed. In section II, cyber crime is detailed along with its two classifications of forms of crimes. In section III different types of attacks are briefly overviewed. In the next section, section IV, category of hackers is acknowledged. Then cyber crime's impact is detailed in section V. Last section that is section VI, there is a short overview of cyber security is organized.

WHAT IS CYBER CRIME?

Sussman and Heuston initial planned the term "Cyber Crime" within the year 1995. "Cyber Crime" are the offenses or crimes that take place over electronic communications or data systems. These styles of crimes are primarily the illegitimate activities within which a computer and a network are concerned. Due of the development of the net, the volumes of the cybercrime activities also are increasing as a result of once committing a criminal offense, there's not a desire for the physical gift of the criminal.

Introducing Viruses, Worms, Torjan etc

Anyone who introduces any type of malicious programs that can gain access to other's device while not victim's permissions, provisions applicable for such offences square measure underneath Section 63, Section 66, Section 66A of the IT Act and Section 426 of the IPC.

Cyber pornography

Though pornography is illegal in some countries, it is can be thought-about because the largest business on the internet. Provisions Applicable for such crimes square measure under Section 67, Section 64A and Section 67B of the IT Act.

Source code theft Provisions

Applicable for such crimes square measure underneath Section 43, Section 66 and Section 66B of the IT Act [12].

TYPES OF HACKERS

Any criminals or hackers are usually engineers, doctors, Non technical students etc all educated people who tries to gain the access of other's system.

These are three type of hacker:

White Hat Hackers

They are ethical hackers who basically focus on securing and protecting IT systems. White hat hackers are those who attempts to break into network or system in order to help the holder of the system by making an effort to aware them of the security flaws. Many such kind of people are employed by the companies concerning about the computer security; these are professional sneakers and the collective group of them are often categorized as tiger teams.

Black Hat Hackers

An individual who compromises with the security of computer system without any acknowledgement from the authorized party. They uses their knowledge to exploit the systems.

Grey Hat Hackers

A Grey Hat Hacker is considered as a skilled hacker in the security community who at times acts legally, and sometimes not. They are considered as hybrid between black and white hat hackers. They basically do not hack with the malicious intentions.

IMPACT OF CYBER CRIMES ON ECONOMY

People today are highly dependent on computers, and the internet for money transfers and makes payments. Therefore, the risk of being subjected to online money frauds is extremely high. Norton Cybercrime disclosed in 2011 that over 74 million people in the United States were victims of cybercrime in 2010, which directly resulted in financial losses of approximately $32 billion. Even in India, with the emergence and popularity of "cashless India", chances of being duped online are also increasing, if one is not smart enough to use safe online transaction platforms and apps. Not just individuals suffer from financial losses due to cybercrime; some of the surveys conducted have stated that approximately 80% of the companies participating in the surveys accepted financial losses due to cybercrime.

CRIME AGAINST PEOPLE

In this, the criminal provides numerous false promotions and gives the people an illusion of security by forcing them to administer their personal information. It includes child pornography, a dominant offence. Social networking sites and the chat groups can also be concluded as a serious cyber crime at times.

CRIME AGAINST PROPERTY

Criminals can easily with their techniques steal the personal information of the other people computer system and the theft gains the unauthorized access to an internet connection, can be a cyber crime.

CRIME AGAINST BUSINESS

In this crime, criminal basically hacks the system or machine of any business organization; They store and steal the confidential and the sensitive data of the system on the server. They acquire unauthorized access to the secured and confidential data of the company and via this, they transfer fund's of the company to their accounts that makes the organization bankrupt.

CRIME AGAINST GOVERNMENT CYBER

Terrorism is a term used against government crime in which hackers hacks the secured and confidential database of the government with the urge to use sensitive and personal information of the Government that reduces the faith of the citizens.

CYBER SECURITY

A branch of technology essentially called cyber security or info security applied to networks and computers. The objective carries' protection {of data of knowledge of info} or information, and also the property from the thefts, natural disaster, or corruption, and permitting the property and data to stay productive and accessible to its users. The Cyber security implies to the processes, and also the technologies that square measure designed to safeguard networks, computers, and also the knowledge from the unauthorized access, attacks, and vulnerabilities delivered via the net by cyber criminals.

Prevention tips for cyber crime

- Do Keep your firewalls (infrastructure defense systems) up so far
- . certify that your system is organized safely and firmly.
- Invariably opt for sturdy passwords and security checks for social networking sites, email boxes, and for your systems.
- Don't answer unknown mails.
- shield your system with some securities package
- Defend or shield your personal info from unknown folks or strangers.
- Safe browsing, and do maintain some sensible system hygiene.
- Keep change your passwords, and login id is a minimum of once or doubly in one or 2 months and create them sturdy.
- Do shield your knowledge and private info and avoid being scammed.
- Never send personal info and knowledge via mail or the other suggests that.
- Create your system clean time to time and review your social media sites as well

WHAT IS CYBER LAW?

The Cyber law is the part of overall legal system which deals with Internet, cyberspace, and their respective legal issues. It covers enough broad area, also covering several subtopics including freedom of expression(Article 9 of Indian Constitution) access to and usage of the Internet, and online privacy. cyber law is referred as the Law of the Internet.

The first cyber law was the Computer Fraud and Abuse Act, was enacted in 1986.This is Known as CFAA. This law prohibits the unauthorized access to computers and it also includes detail about the levels of punishment for breaking that law.

WHY ARE CYBER LAWS NEEDED?

Like any law, the cyber law is also created to protect people and the organizations on the Internet from malicious people and help to maintain law and order. If someone breaks a cyber law or rule, it allows another person or organization to take action against another person or have them sentenced to a punishment.

IMPORTANCE OF CYBER LAW

- It covers all transaction that happens on the internet.
- It keeps eyes on all activities that happens on the internet.
- It touches every action and every reaction in the cyberspace.

AREA OF CYBER LAW

Cyber laws contain different types of purposes. Some of the laws create rules for how the individuals, and the companies may use computers , and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet.

The major areas of cyber law include:

Fraud: Consumers depend on the cyber laws to protect them from online fraud. Laws are made to prevent the identity theft, credit card theft, and other financial crimes that happen online. The person who commits identity theft may face confederate or state criminal charges. He /she might also encounter a civil action brought by the victim. The cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

Copyright: Copyright violation is an area of cyber law that protects the rights of the individuals, and the companies to profit from their own creative works. The internet has made the copyright violations easier. In back days of online communication, copyright violations was too easy. Both the companies, and the individuals need lawyers to bring actions to impose copyright protections.

Defamation: Several personnel use the net to talk their mind. Once folks use the net to mention things that don, 't seem to be true in nature, it will cross the road into defamation. Defamation laws are the civil laws that save people from faux public statements which might damage any business, or someone's personal name. Once folks use the net to form such statement.

Harassment and Stalking: Sometimes online statements will violate criminal laws that forbid harassment and stalking. Once an individual makes threatening statements once more and once more concerning some other person online, there's violation of each civil and criminal laws. Cyber lawyers each prosecute and defend individuals once stalking happens mistreatment the web and different types of the transmission.

Freedom of Speech: Freedom of speech is a crucial space of cyber law. Although cyber laws forbid bound behaviors online, freedom of speech laws conjointly permit folks to talk their minds. Cyber lawyers should advise their shoppers on the bounds of free speech as well as laws that require obscenity. Cyber lawyers might also defend their shoppers once there's a dialogue regarding whether or not their actions comprise permissible free speech.

Trade Secrets: Companies doing businesses online usually rely on cyber laws to safeguard their trade secrets. For instance, Google and alternative online search engines pay several times developing the algorithms that turn out search results. They additionally pay a good deal of your time developing alternative options like maps, intelligent help and flight search services to call a couple of. Cyber laws facilitate these firms to require proceeding as necessary to safeguard their trade secrets.

Contracts and Employment Law: Every time you click a button that claims you comply with the terms, and conditions of employing a website, you've got used cyber law. There area unit terms and conditions for each website that area unit somehow associated with privacy Considerations.

PENALTIES AND OFFENCES

Cyber Crime	Brief Description	Relevant Section in IT Act	Punishments
Cyber Stalking	Stealthily following a person, tracking his internet chats.	43, 65, 66	3 years, or with fine up to 2 lakh
Cyber Pornography including child pornography	Publishing Obscene in Electronic Form involving children	67, 67 (2)	10 years and with fine may extends to 10 lakh
Intellectual Property Crimes	Source Code Tampering, piracy, copyright infringement etc.	65	3 years, or with fine up to 2 lakh
Cyber Terrorism	Protection against cyber terrorism	69	Imprisonment for a term, may extend to 7 years
Cyber Hacking	Destruction, deletion, alteration, etc in a computer resources	66	3 years, or with fine up to 2 lakh
Phishing	Bank Financial Frauds in Electronic Banking	43, 65, 66	3 years, or with fine up to 2 lakh
Privacy	Unauthorized access to compute	43, 66, 67, 69, 72	2 years, or with fine upto 1 lakh

CYBER LAW (IT LAW) IN INDIA

Cyber Law additionally known as IT Law is the law relates to Information-technology as well as computers and web. It's associated with legal science and supervises the digital circulation of knowledge, software, data security and e-commerce. IT law doesn't consist a separate space of law rather it encloses aspects to contract, holding, privacy, and knowledge protection laws. Holding could be a key part of IT law. The world of software package license is moot and still evolving in Europe and elsewhere.

THE INFORMATION TECHNOLOGY ACT OF INDIA, 2000

According to Wikipedia "The data Technology Act, 2000 (also referred to as ITA-2000, or the IT Act) is an act of the Indian Parliament (no twenty-one of 2000), it was notified on 17th OCTOBER, 2000. It's the foremost vital law in India that deals with digital crimes or cyber crimes and electronic commerce. It's supported the world organization Model Law on Electronic Commerce, 1996 (UNCITRAL Model) counseled by the final Assembly of United Nations by a resolution dated thirty Jan 1997" .

The I.T. Act, 2000 defines the terms −

- access in computer network in **section 2(a)**
- computer in **section 2(i)**
- computer network in **section (2j)**
- data in **section 2(0)**
- information in **section 2(v)**

Some key points of the data Technology (IT) Act 2000 area unit as follows:

- E-mail is currently thought of as a legitimate and legal kind of communication.
- Digital signature's area unit given legal validity among the Act.
- Act has born to new business to firms to issue digital certificates by changing into the Certifying Authorities.

- This Act permits the government to issue notices on the internet through e-governance.
- The communication between the businesses or between the company, and therefore, the government may be done through internet.
- Addressing the problem of security is the most significant feature of this Act. It introduced the construct of digital signatures that verify the identity of a private on the internet.
- just in case of any damage or loss done to the corporate by the criminals, the Act provides a remedy within the kind of money to the corporate.

Salient features of the information Technology (Amendment) Act, 2008

The term 'digital signature' has been replaced with 'electronic signature' to form the Act a lot of technology neutral. A new section has been inserted to outline, 'communication device' to mean cell phones, personal digital help or combination of each or the other device accustomed to communicate, send or transmit any text video, audio or image. A new section has been added to outline cyber restaurant as any facility from wherever the access to the net is obtainable by any person within the standard course of business to the members of the public. New Section to deal with information protection and privacy -Section 43 Body company to implement the best security practices-Sections 43A &72A

CYBER CRIME'S SCENARIO IN INDIA

1.CYBER TERRORIST ACT

Since the changes were administrated within the info Technology Act in city, this case of cyber terrorist act was its initial project. A threat email had been delivered to the BSE and NSE, at 10:44 am on Mon. With the MRA Marg police, and therefore, the Cyber Crime Investigation Cell (CCIC) operating along on the cyber crime case, the defendant has been detained. The information science address had been derived from Patna, Bihar. Once checked for any personal details, 2 contact numbers were found, that belonged to a photograph frame maker in Patna.

2.BAZEE.COM CASE

CEO of Bazee.com was inactive in Gregorian calendar month 2004 as a result of a CD with objectionable material was being sold on the website. The CD was conjointly being sold within the markets in the city. The Bombay Police and also the city Police got into action. The business executive was later discharged on bail. This opened the question on what quite distinction we have a tendency to draw between net Service supplier and Content supplier. The burden rests on the suspect that he was the Service supplier and not the Content supplier. It conjointly raises loads of problems concerning however, the police ought to handle crime cases.

3.ANDHRA PRADESH TAX CASE

Dubious ways of a distinguished man of affairs, from province, were exposed once officers of the department got hold of computers, employed by the suspect in one among the various cyber fraud cases in Asian country. The owner of a plastics firm was inactive and Rs twenty two large integer money, was recovered from his house by sleuths of the Vigilance Department. They sought-after a proof from him concerning the unaccounted money among ten days. The suspect submitted half-dozen,000 vouchers, to prove the legitimacy of trade and thought his offence would go unobserved however once careful scrutiny of vouchers and contents of his computers, it had been disclosed that every one of them were created once the raids were conducted. It had been later disclosed that the suspect was running 5 businesses below the pretense of 1 company and used faux and processed vouchers to point out sales records and save tax.

PERSONAL CASES

Cyber Police has in remission a Husband for misusing his wife's FB account, in an exceedingly cyber case in India. He employed AN moral hacker to hack into his wife's FB account in order that he will notice items of proof concerning her unhealthy character.

Using the Trojan or malware, a woman's digital camera was accessed to capture her non-public videos, And announce on an outlawed website. The incident came into light-weight once the metropolis resident appeared for an interview.

The cyber fraud case of duplication of a SIM card was registered with the police once a man of affairs from Ahmedabad caught wind of it. He registered a grievance beneath the cyber and money crime since the defrauders had submitted faux documents with the mobile company to realize the businessman's personal details

. In a social media connected law-breaking grievance, a famed Gujarati singer claimed that her photos were getting used by an unknown man, locution they were married and had a baby along.

To gain personal revenge, AN ex-boyfriend, operating as a programmer, announce his ex's personal telephone number on a 24×7 chemical analysis service helpline, was in remission in an exceedingly leading law-breaking case.

WHAT HAPPENS IF YOU BREAK A CYBER LAW?

There area unit totally different styles of social control reckoning on the sort of cyber law you bust, United Nations agency you displeased, wherever you bust the law, and wherever you reside. In several things, breaking the principles on an internet site end in your account turning into suspended or prohibited, and your informatics self-addressed blocked. To see the results of your action for minor offenses, we tend to advocate reviewing the businesses terms of service or rule. If you have committed a lot of serious offense like hacking, offensive another person or website, or inflicting another person or company distress, further action is also taken against you.

CONCLUSION

The rise and proliferation of fresh developed technologies begin star to control several cybercrime in recent years. Crime has become nice threats to mankind. Protection against crime could be a very important half for social, cultural and security facet of a rustic. The Government of India has enacted IT Act, 2000 to subsume cybercrime. The Act any revise the IPC, 1860, the IEA (Indian proof Act), 1872, the Banker's Books proof Act 1891 and therefore, the banking company of India Act, 1934. Any part of the planet cyber crime might be originated passing national boundaries over the web making each technical and legal complexities of the work and prosecuting these crimes. The international harmonizing efforts, coordination and co-operation among varied nations square measure needed to require action towards the cyber crimes.