International Journal of Research in Engineering, Science and Management
Volume 4, Issue 7, July 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

Cyber Crime: Are the Law Outdated for this Type of Crime

Divy Shivpuri*
Student, Law College, Uttaranchal University, Dehradun, India

***Abstract*: Cybercrime can be defined as an "illegal act in which a computer is a tool or a goal or both". Late, the use of computers has become extremely common and popular. However, the misuse of technology in cyberspace has led to cybercrime both nationally and internationally. With the intention of regulating criminal activities in the cyber world and protecting the technological advancement system, the Indian parliament approved the law on technological information, 2000. It was the first global law of India to deal with technology in the field of e-commerce, e-governance, electronic banking services, as well as penalties and punishments regarding computer crimes. This paper mainly deals with the laws relating to the cyber-crimes in India. The objectives of this research paper to analyse the concept of cyber-crime in India and give suggestions to make the laws more effective to deal with it.**

***Keywords*: cyber-crime.**

1. Introduction

The invention of Computer has made the life of humans easier; it has been using for various purposes starting from the individual to large organizations across the globe. In simple term we can define computer as the machine that can stores and manipulate/process information or instruction that are instructed by the user. Most computer users are utilizing the PC for the erroneous purposes either for his or her personal benefits or for other's benefit since decades. This gave birth to "Cyber Crime". This had led to the engagement in activities which are illegal to the society. We can define Cyber Crime because the crimes committed using computers or network and are usually happen over the cyber space especially the web.

Presently comes the expression "Cyber Law". It doesn't have a fixed definition, however in a basic term we can characterized it as the law that oversees the cyberspace. Cyber laws are the laws that oversee cyber area. Cyber Crimes, computerized and electronic marks, information securities and securities and so on are understood by the Cyber Law. The UN's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL) Model [1].

Computer crimes include criminal activities carried out using computers that further perpetrate crimes such as phishing, counterfeiting, cyber-bullying, pornography, bombardment of e-mails, spam, sale of illegal articles, etc. Although cyber-crime has its general meaning as "A legal error which will be followed by criminal proceedings which will end in punishment".

2. Objective

The rule focus of our paper is to spread the information on the crimes or offenses that occur through the web or the cyberspace, alongside the laws that are forced against those crimes and lawbreakers. We are additionally trying to specialize in the security in cyberspace. Further, we will look on the laws that are outdated for this type of crime and try to give some suggestions for making them effective.

3. Cyber Crime and Cyber Law

We can define "Cyber Crime" as any malefactor or other offences where electronic communications or information systems, including any device or the web or both or more of them are involved and "Cyber law" as the legal issues that are related to utilize of communications technology, concretely "cyberspace", i.e., the Internet. It is an endeavour to integrate the challenges presented by act on the web with legacy system of laws applicable to the physical world.

A. Cyber Crime and its History

Sussman and Heuston initially proposed the expression "Cyber Crime" in the year 1995. Cybercrime can't be portrayed as a solitary definition; it is best considered as an assortment of acts or directs. These demonstrations depend on the material offense object that influences the computer information or frameworks. These are the illicit demonstrations where an advanced gadget or data framework is an apparatus or an objective or it tends to be the mix of both. The cybercrime is otherwise called electronic crimes, computer-related crimes, e-crime, high innovation crime, data age crime and so on.

In straightforward term we can portray "Cyber Crime" are the offenses or crimes that happens over electronic correspondences or data frameworks. These sorts of crimes are essentially the criminal operations in which a computer and a network are included. Due of the improvement of the web, the volumes of the cybercrime exercises are additionally expanding in light of the fact that when perpetrating a crime there could be not, at this point a requirement for the actual present of the crook.

The strange quality of cybercrime is that the person in

*Corresponding author: divyshivpuri@gmail.com

question furthermore, the wrongdoer may never come into direct contact. Cybercriminals regularly pick to work from nations with non-existent or powerless cybercrime laws to lessen the odds of location and indictment.

There is a myth among the people that cybercrimes can only be committed over the cyberspace or the internet. In fact, cybercrimes can also be committed without one's involvement in the cyber space, it is not necessary that the cyber criminal should remain present online. Software privacy can be taken as an example.

1) History of cyber crime

The first Cyber Crime was recorded within the year 1820. 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 so as to discourage Jacquard so that the new technology cannot be utilized in the future.

Table 1

1997	Cybercrimes and viruses initiated, that includes Morris Code worm and other
2004	Malicious code, Torjan, Advanced worm etc. 2007 Identifying thief, Phishing etc
2010	DNS Attack, Rise of Botnets, SQL attacks etc
2013	Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransomware attack etc
present	Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Android hack, Cyber warfare etc.

2) Classification of Cyber Crime

Cyber Crime can be classified into four major categories. They are as follows:

a) Cyber Crime against individuals: Crimes that are committed by the cyber criminals against an individual or a person. A few cybercrimes against individuals are:

- Email spoofing: This technique is a forgery of an email header. This means that the message appears to possess received from someone or somewhere aside from the real or actual source. These tactics are usually used in spam campaigns or in phishing, because people are probably going to open an electronic mail or an email when they think that the email has been sent by a legitimate source.
- Spamming: Email spam which is otherwise called as junk email. It is unsought mass message sent through email. The uses of spam have become popular in the mid-1990s and it is a problem faced by most email users now a days. Recipient's email addresses are obtained by spam bots, which are automated programs that crawls the web in search of email addresses. The spammers use spam bots to make email distribution lists. With the expectation of receiving a few numbers of respond a spammer typically sends an email to millions of email addresses.
- Cyber defamation: Cyber defamation means the harm that's brought on the reputation of a private within the eyes of other individual through the cyber space. The purpose of making defamatory statement is to bring down the reputation of the individual.
- IRC Crime (Internet Relay Chat): IRC servers allow the people round the world to return together under one platform which is sometime called as rooms and that they chat to each other. Cyber Criminals basically uses it for meeting. Hacker uses it for discussing their techniques. Paedophiles use it to allure small children.

A few reasons behind IRC Crime: Chat to win one's confidence and later starts to harass sexually, and then blackmail people for ransom, and if the victim denied paying the amount, criminal starts threatening to upload victim's nude photographs or video on the internet.

  - A few are paedophiles, they harass children for his or her own benefits.
  - A few uses IRC by offering fake jobs and sometime fake lottery and earns money [2].
- Phishing: In this type of crimes or fraud the attackers try 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. Some other cybercrimes against individuals includes Net extortion, Hacking, public nudity, Trafficking, Distribution, Posting, master Card, Malicious code etc. The potential harm of such a malefaction to a private person can scarcely be bigger.

b) 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:

- Software piracy: It can be describing as the copying of software unauthorizedly.
- 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 unauthorizedly such as music, software, text etc.
- Trademark infringement: It are often described because the using of a service mark or trademark unauthorizedly.

c) Cyber Crime against organization: Cyber Crimes against organization are as follows:

- Unauthorized changing or deleting of data.
- Reading or copying of tip unauthorizedly, but the info are neither being change nor deleted.
- DOS attack: During this attack, the attacker floods the servers, systems or networks with traffic in order to overwhelm the victim resources and make it infeasible or difficult for the users to use them.
- Email bombing: It's a kind of Net Abuse, where huge numbers of emails are sent to an email address in order to overflow or flood the mailbox with mails or to flood the server where the e-mail address is.
- Salami attack: The other name of Salami attack is Salami slicing. In this attack, the attackers use a web database so

as to seize the customer's information like bank details, master card details etc. Attacker deduces very little amounts from every account over a period of your time. In this attack, no complaint is file and the hackers remain free from detection as the clients remain unaware of the slicing. Some other cybercrimes against organization includes Logical bomb, Torjan horse, Data diddling etc.

d) Cyber Crime against society: Cyber Crime against society includes:

- Forgery: Forgery means making of false document, signature, currency, stamp etc.
- Web jacking: The term Web jacking has been derived from hi jacking. In this offence the attacker creates a fake website and when the victim opens the link a replacement page appears with the message and that they got to click another link. If the victim clicks the link that appears real, he is going to be redirected to a fake page. These types of attacks are done to get entrance or to get access and controls the site of another. The attacker may also change the information of the victim's webpage.

3) Cyber Crime's scenario in India

a) The Bank NSP Case

In this case a management trainee of a bank got engaged to a wedding. The couple wanted to exchange many emails using the company's computers. After a while, that they had choppy their marriage and therefore the girl created some fake email ids like "Indian bar associations" and sent mails to the boy's foreign clients. She used the banks computer to try to do. The boy's company lost an enormous number of clients and took the bank to court. The bank was held responsible for the emails sent using the bank's system.

b) SONY.SAMBANDH.COM case

India saw its 1st cybercrime conviction. This is often the case where Sony India Private Limited filed a complaint that runs an internet site mentioned as www.sony-sambandh.com targeting the NRIs. The website allows NRIs to send Sony products to their friends and relatives in India after they buy it online. The corporate undertakes to deliver the products to the involved recipients. In May 2002, somebody logged onto the online site underneath the identity of Barbara Campa and ordered a Sony color television set and a cordless head phone. She requested to deliver the merchandise to Arif Azim in Noida and gave the number of her credit card for payment. The payment was accordingly cleared by the credit card agency and the transaction processed. After the related procedures of dues diligence and checking, the items were delivered to Arif Azim by the company. When the product was delivered, the company took digital pictures so as to indicate the delivery being accepted by Arif Azim. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase. The company had filed a complaint for online cheating at the CBI that registered a case under the Section 418, Section 419 and Section 420 of the IPC (Indian Penal Code). Arif Azim was arrested after the matter was investigated. Investigations discovered that Arif Azim, whereas acting at a call centre in Noida did gain access to the number of the credit card of an American national which he misused on the company's site. The CBI recovered the color television along with the cordless head phone. In this matter, the CBI had proof to prove their case so the accused admitted his guilt. The court had convicted Arif Azim under the Section 418, Section 419 and Section 420 of the IPC, this being the first time that a cybercrime has been convicted. The court, felt that since the defendant was a boy of 24 years and a firsttime convict, a compassionate view needed to be taken. Thus, the court discharged the defendant on the probation for one year.

Some, Section 67 and Section 70 of the IT Act are also applied. In this case, the hackers hacks ones webpage and replace the homepage with pornographic or defamatory page.

c) Bazee.com case

In December 2004 the Chief Executive Officer of Bazee.com was arrested because he was selling a compact disk (CD) with offensive material on the website, and even CD was also conjointly sold-out in the market of Delhi. The Delhi police and therefore the Mumbai Police got into action and later the CEO was free on bail.

d) Parliament Attack Case

The Bureau of Police Research and Development, Hyderabad had handled this case. A laptop was recovered from the terrorist who attacked the Parliament. The laptop which was detained from the two terrorists, who were gunned down on 13th December 2001 when the Parliament was under siege, was sent to Computer Forensics Division of BPRD. The laptop contained several proofs that affirmed the two terrorist's motives, mainly the sticker of the Ministry of Home that they had created on the laptop and affixed on their ambassador car to achieve entry into Parliament House and the fake ID card that one of the two terrorists was carrying with a Government of India emblem and seal. The emblems (of the 3 lions) were carefully scanned and additionally the seal was also craftly created together with a residential address of Jammu and Kashmir. However careful detection proved that it was all forged and made on the laptop.

e) Andhra Pradesh Tax Case

The owner of the plastics firm in Andhra Pradesh was arrested and cash of Rs. 22 was recovered from his house by the Vigilance Department. They wanted evidence from him concerning the unaccounted cash. The suspected person submitted 6,000 vouchers to prove the legitimacy of trade, however when careful scrutiny the vouchers and contents of his computers it unconcealed that every one of them were made after the raids were conducted. It had been concealed that the suspect was running 5 businesses beneath the presence of 1 company and used fake and computerized vouchers to show sales records and save tax. So the dubious techniques of the businessman from the state were exposed when officials of the department got hold of computers utilized by the suspected person.

B. Cyber Law

Cyber Law took birth in order to take control over the crimes committed through the internet or the cyberspace or through the uses of computer resources. Description of the lawful issues

that are related to the uses of communication or computer technology can be termed as Cyber Law.

1) What is the importance of Cyber Law?

Cyber law plays a very important role in this new epoch of technology. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, but each action and each reaction in Cyberspace has some legal and Cyber legal views.

2) The Information Technology Act of India, 2000

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000), it was notified on 17th October 2000. It is the most important law in India that deals with the digital crimes or cybercrimes and electronic commerce. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

Some key points of the Information Technology (IT) Act 2000 are as follows:

- E-mail is now considered as a valid and legal form of communication.
- Digital signatures are given legal validity within the Act.
- Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on internet through e-governance.
- The communication between the companies or between the company and the government can be done through internet.
- Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.
- In case of any harm or loss done to the company by criminals, the Act provides a remedy in the form of money to the company [3].

4. Cyber Law in India

Following are the sections under IT Act, 2000

1) Section 65: Temping with the computers source documents

Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program, and computer system or computer network.

Punishment: Any person who involves in such crimes could be sentenced up to 3 years imprisonment or with a fine of Rs.2 lakhs or with both.

2) Section 66: Hacking with computer system, data alteration etc.

Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking.

Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment, or with a fine that may extend upto 2 lakhs rupees, or both [16].

3) Section 66A: Sending offensive messages through any communication services

- Any information or message sent through any communication services this is offensive or has threatening characters.
- Any information that is not true or is not valid and is sent with the end goal of annoying, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will.
- Any electronic mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive the address about the origin of the messages.

Punishment: Any individual found to commit such crimes under this section could be sentenced upto 3years of imprisonment along with a fine.

4) Section 66B: Receiving stolen computer's resources or communication devices dishonestly Receiving or retaining any stolen computer, computer's resources or any communication devices knowingly or having the reason to believe the same.

Punishment: Any person who involves in such crimes could be sentenced either description for a term that may extend upto 3 years of imprisonment or with a fine of rupee 1 lakh or both.

5) Section 66C: Identify theft Using of one's digital or electronic signature or one's password or any other unique identification of any person is a crime.

Punishment: Any person who involve in such crimes could be sentenced either with a description for a term which may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

6) Section 66D: Cheating by personation by the use of computer's resources

Whoever tries to cheats someone by personating through any communication devices or computer's resources shall be sentenced either with a description for a term that may extend upto 3 years of imprisonment along with a fine that may extend upto rupee 1 lakh.

7) Section 66E: rivacy or violation

Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violets the privacy of the individual shall be shall be sentenced to 3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both.

8) Section 66F: Cyber terrorism

A. Whoever intentionally threatened the integrity, unity, sovereignty or security or strike terror among the people or among any group of people by,
   I. Deny to any people to access computer's resources.
   II. Attempting to break in or access a computer resource without any authorization or to exceed authorized access.
   III. Introducing any computer's contaminant, and through such conducts causes or is probable to cause any death or injury to any individual or damage or

any destruction of properties or disrupt or it is known that by such conduct it is probable to cause damage or disruptions of supply or services that are essential to the life of people or unfavourably affect the critical information's infrastructure specified under the section 70 of the IT Act.

B. By intention or by knowingly tries to go through or tries to gain access to computer's resources without the authorization or exceeding authorized access, and by such conducts obtains access to the data, information or computer's database which is limited or restricted for certain reason because of the security of the state or foreign relations, or any restricted database, data or any information with the reason to believe that those data or information or the computer's database obtained may use to cause or probably use to cause injury to the interest of the independence and integrity of our country India.

Punishment: Whoever conspires or commits such cyber-crime or cyber terrorism shall be sentenced to life time imprisonment.

9) Section 67: Transmitting or publishing obscene materials in electronic form

Whoever transmits or publishes or cause to publish any obscene materials in electronics form. Any material that is vulgar or appeal to be lubricious or if its effect is for instance to tends to corrupt any individual who are likely to have regard to all relevant circumstances to read or to see or to hear the matter that contained in it, shall be sentenced on the first convict with either description for a term that may extend upto five years of imprisonment along with a fine which may extend upto 1 lakh rupee and in the second or subsequent convict it can be sentenced either description for a term that may extend upto ten years along with a fine that may perhaps extend to two lakhs rupees.

10) Section 67A: Transmitting or publishing of materials that contains sexually explicit contents, acts etc. in electronics form

Whoever transmits or publishes materials that contains sexually explicit contents or acts shall be sentences for either description for a term which may extend upto 5 years or imprisonment along with a fine that could extend to 10 lakhs rupees in the first convict. And in the event of the second convict criminal could be sentenced for either description for a term that could extend upto 7 years of imprisonment along with a fine that may extend upto 20 lakhs rupees.

11) Section 67B: Transmitting or publishing of materials that depicts children in sexually explicit act etc in electronics form

Whoever transmits or publishes any materials that depict children in sexually explicit act or conduct in any electronics form shall be sentenced for either description for a term which may extend to 5 years of imprisonment with a fine that could extend to rupees 10 lakhs on the first conviction. And in the event of second conviction criminals could be sentenced for either description for a term that could extend to 7 years along with a fine that could extend to rupees 10 lakhs.

12) Section 67C: Retention and preservation of information by intermediaries

I. Intermediaries shall retain and preserve such information that might specify for such period and in such a format and manner that the Central Government may prescribe.

II. Any intermediaries knowingly or intentionally contravene the provision of the sub-section. Punishment: Whoever commits such crimes shall be sentenced for a period that may extend upto 3 years of imprisonment and also liable to fine.

13) Section 69: Power to issue direction for monitor, decryption or interception of any information through computer's resources

I. Where the Central government's or State government's authorized officers, as the case may be in this behalf, if fulfilled that it is required or expedient to do in the interest of the integrity or the sovereignty, the security defence of our country India, state's security, friendly relations with the foreign states for preventing any incident to the commission of any cognizable offences that is related to above or investigation of any offences that is subjected to the provision of sub-section (II). For reasons to be recorded writing, direct any agency of the appropriate government, by order, decrypt or monitor or cause to be intercept any information that is generated or received or transmitted or is stored in any computer's resources.

II. The safeguard and the procedure that is subjected to such decryption, monitoring or interception may carry out, shall be such as may be prescribed.

III. The intermediaries, the subscribers or any individual who is in the charge of the computer's resources shall call upon by any agencies referred to the sub-section (I), extends all services and technical assistances to:

a) Providing safe access or access to computer's resources receiving, transmitting, generating or to store such information or

b) Decrypting, intercepting or monitoring the information, as the case might be or

c) Providing information that is stored in computer. IV. The intermediaries, the subscribes or any individual who fails to help the agency referred in the sub-section (III), shall be sentenced for a term that could extend to 7 years of imprisonment and also could be legally responsible to fine.

5. Laws are Outdated for Cybercrimes

In this developing era, the utilization of internet is paced up to an excellent extent and with this increase in its use, offenses involving the IT Sector have also increased substantially. After 1991 when the new policy was introduced by the government, the IT Sector flourished and lots of people were engaged and employed. This growth, though, solved variety of issues concerning employment and exchange but since then, more and more cases are reported by the people which especially include E-mail frauds, wrongful transactions, hacking of the accounts etc.

In order to beat these problems, it had been essential to determine a legal framework which may affect such situations. the start of this framework are often spotted within the year

2000 when the knowledge Technology Act was introduced for the primary time although, specific information on what's meant by cyber-crimes wasn't mentioned within.

The IT Act includes the principles and regulations of the electronic governance, establishment of a board of securities with certain powers and functions to perform, categorization of the offenses covered under the ambit of cybercrimes, authorization of certain bodies etc. The IT Act, 2000 as amended in 2008 acts because the most vital statute in handling cybercrimes in India.

The laws that currently run the judiciary were made quite a century ago and therefore the development of the cyber-crimes have made these laws ineffective in certain ways. The motive of the then made laws was to curb with the traditional issues and not with the recently developed special problems just like the cyber-crimes and this had led to a big increase within the rate of those crimes.

Also, due to the less developed technology on the official front, the offenders are largely unreachable showcasing the incapability of the present laws. Lack of skilled personnel and scarcity of trainings during this field is additionally a crucial issue.

The terrorist organizations nowadays attempt to use different hacking techniques so as to access confidential data of the governmental organizations and execute their plans. Such acts also are covered under the ambit of cyber-crimes and increase the quantum of those offenses.

From the start of the 21st century, IT Act has been the sole Act which protects a private or a corporation from these sorts of crimes and lays down the punishments for an equivalent. Sufficiency of laws are often guaranteed on the idea that the associated crimes are reduced after the enactment of the laws but this can't be observed during this case. the speed of cyber-crimes has been increased exponentially within the past 20 years.

The field of digital forensics which may be considered as a crucial a part of the cyber investigations has been unexplored in India. Secondly, the concerned officers must be told that the materials that are gathered while investigation of cyber-crimes is sensitive in nature and must be handled carefully.

6. Conclusion

Many international treaties dealing with cybercrime have been developed. As far as we can tell, the overall growth of the establishment is in contrast to existing multilateral and regional legal instruments, as well as many national laws, and it is based on investigation measures and powers related to digital evidence, regulation, risk, and jurisdiction, as well as international cooperation. As we broaden the scope of their applicability, these types of treaties also differ geographically. This border creates a number of barriers for effective cybercrime investigation, identification, and procedure, as well as the prevention of cybercrime.

According to my understanding, the large wall has weak sanctions and low deterrence. The punishments do not take into account the effects that cybercrime might have on an individual's life. Penalties have yet to be revised to reflect the large-scale economic and social effects on society and individuals.

The primary purpose of this publication is to distribute cybercrime information to the general public. We mean that cybercrime can never be recognized at the end of this text "A Brief Study on Cyber Crime and Cyber Law in India." If someone falls victim to a cyber-attack, submit a report with the local police station. Criminals will never stop if they are not penalized for their actions.

References

[1] http://www.academia.edu/7781826/IMPACT_OF_SOCIAL_MEDIA_ON_SOCIETY_and_CYBER_LAW
[2] http://ccasociety.com/what-is-irc-crime/
[3] https://www.ijarcsse.com/docs/papers/Volume_5/8_August2015/V5I8-0156.pdf