IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

An Overview: On Cyber Crime and Cyber Law's in India

Dr. Kamlakar Eknath Kamble
Associate Professor, Department of Commerce & HoD
KES's Dr. C. D. Deshmukh Commerce & Sau. K. G. Tamhane Arts College, Roha, Raigad, India
kamlakar19752@gmail.com

Abstract: *Using Internet, the computer-based facilities the worldwide connection of loosely held networks. Network facilities such as Internet, Internet Banking, Online Transaction, Online Mobile Phones Usually chat and WhatsApp, Pictures, Music and other facilities has become the regular requirements of the large of people in India. Today's modern environment or scenario, huge number of people are using such innovative Tools or equipment's and they considered it very essential or necessary in todays wide world without which their life is incomplete. Now a few days some peoples and groupof peoples used internet for criminal activities, like unauthorized access to others networks, fraud, scams etc. These criminal activities related to the internet are referred as Cyber Crime. Cyber-crime refers to all the activities done with criminal internet in cyberspace. Today day by day increasing popularity of Online activities like as online shopping, online Banking etc. When the web is used on the worldwide stage, everyone can access the resources of the internet from anywhere, any time every one from every corner, of the world. Some peoples are using wrong methods of using the internet technology by some peoples for criminal activities. These criminal act or activities, or the Crimes/offence connected to with the internet is treated as Cybercrime. The term "In order to stop or to punish the cyber-Criminals the concept is "Cyber Law" is introduced.* ***Cyber Law can be defined as law of the web****. Several law rules and methods has been introduced in order to control or prevent cybercrime and the punishments and penalties are laid down to the criminals. Therefore, keeping the objectives in the mind this study is divided in to different clause and sections. Cybercrimes may be various dimensions affecting not only in the business, the persons, property, reputation, state etc. many times force of the law enactors not only make the laws but also needed the proper counselling and monitoring authorities to handle and control such as web activities.*

Keywords: Network, Web, Internet, Cyber Crime, Cyber security, Cyberspace, Criminals. IT etc

I. INTRODUCTION

Today, a computer can be defined as a device, tools, or Machine that stores and process information that are instructed by the users. Cyberspace is the Internet has made the flow of information and data between different networks very easy and more effective. India having the huge population and widespread use ofInternet, Mobile Cells, Computers, and other devices of Information Technology, that is not easy to use, low-cost rates but very fastest method in providing the information required by the person compare with the other modes of technologies and therefore the large number of people are using it. Which again in turns results increase in misuse (Cybercrimes). Cyber Crime such as hacking, bugging, cheating, pornography, Fraud, EmailBombing, data diddling, salami attacks, Virus/worm attacks, logic bombs, Trojan horse, web jacking, Government sites hacking etc., has become so popular on the internet. Any criminal activity that involves a computer, networked device, or any other related device can be considered a cybercrime. There are some instances when cybercrimes are carried out with the intention of generating profit for the cybercriminals, whereas other times a cybercrime is carried out directly to damage or disable the computer or device. It is also possible that others use computers or networks to spread malware, illegal information, images, or any other kind of material. As a result of cybercrime, many types of profit-driven criminal activities can be perpetrated, such as ransomware attacks, email and internet fraud, identity theft, and frauds involving financial accounts, credit cards or any other payment card.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

In India, cybercrimes are covered by the Information Technology Act, 2000 and the Indian Penal Code, 1860. It is the Information Technology Act, 2000, which deals with issues related to cybercrimes and electronic commerce. However, in the year 2008, the Act was amended and outlined the definition and punishment of cybercrime. Several amendments to the Indian Penal Code 1860 and the Reserve Bank of India Act were also made.

Need of Cyber Laws:

Today's Computer-generated world due to the development of Internet is known as cyberspace and the Laws prevailing this web, Internet area are known as Cyber Laws and all the users of this area come under the rules of these Laws it carries a kind of worldwide Jurisdictions. Cyber Law also be described as that branch of law that deals with the legal issues related to use of Internet Network Information Technology. So, the need of Cyber Laws is to protect the web life of users. Day to day Cyber challenges has increased. The Cyber Laws regulate in all the fields of laws in which cybercrimes can be committed, such as contract, intellectual property law, criminal law, and law of tort. Cyber laws deal with various kinds of concerns, such as safety, free speech, privacy, terrorism, E-commerce, Intellectual property rights, and applications of jurisdiction of cyber laws.

Today, increase in the number of internet users, the need of cyber laws and their rules has become very vital in new modern times. The Indian cyber–Crime Laws covers major aspects of cyber space and Cyber-crimes. Cyber laws are needed because:

Almost all consumers and companies extensively depend upon their computers networks and keep their important data in electric form.

Consumers are huge increasingly using credit/debit cards, Internet banking, mobile applications for shopping.

Maximum peoples are using email, phones and SMS Massages for communication.

Digital Signatures and e-contracts are fast growing or replacing conventional methods of business.

All Transactions of Share Markets are in Demat or electronic format.

Almost Government forms including income tax return, company law forms etc. are now filled in electronic form.

Almost online transactions with increased popularity of payment apps and sites, as they are easy and efficient and having financial benefits.

"Cashless India" a Government scheme has also gained popularity resulting in a huge number of online transactions.

Social Media and social networking sites like, Facebook, Instagram, Blogs, WhatsApp's, etc. the main mode of communication. It is become just like a blood in body without which one cannot be alive.

Almost communication of government forms are in electronic form, like a Addhar Card, Pan card, Passport applications, Registration of companies, Digi lockers kept all certificates in electronic form.

Cyber Laws helps in protecting not ons ly individuals but their property and society at large.

Types of Cyber Crime:

In Simple way we can say that cybercrime is unlawful acts wherein the computer is either a tool or a target or both. Cybercrimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000.

Basically, Law has categorized Cybercrimes in two ways:

The Computer as a Target: -using a computer to attack other computers.

Hacking, Virus/Worm attacks attack etc.

computer as a weapon: -using a computer to commit real world crimes.

Cyber Terrorism, IPR violations, Credit card frauds, FT frauds, Pornography etc.

Following Important types of Cyber Crime:

Unauthorised access to computer devices, systems and Networks/ Hacking: This kind of offence is normally treated as hacking in the generic sense.

E-mail bombing- This kind of activity refers to sending large number of mail to the victim, which may be an individual or a company or even mail service their by ultimately resulting into crashing.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

Theft of information contain in electronic form-Theft may be either by appropriating the data physically or by tampering them through the virtual medium.

Child sexually abusive material-This kind of activity include any material containing sexual image in any form in this fact child being exploited or abused may be seen.

A cyberbully- In this type of activity someone who harasses or bullies' others using electronic devices like computers, mobile phones, laptops, etc. Cyberbullying refers to bullying conducted through the use of digital technology. The use of social media, messaging platforms, gaming platforms, and mobile devices may be involved. Oftentimes, this involves repeated behaviour that is intended to scare, anger shame those targeted.

Cyberstalking- This kind of activity harassing or stalking another person online using the internet and other technologies. Cyberstalking is done through texts, emails, social media posts, and other forms.

Cyber Grooming- This type of activity person or the phenomenon of cyber grooming involves a person building a relationship with a teenager and having a strategy of luring, teasing, or even putting pressure on them to perform a sexual act.

Online Job fraud- This kind of offence- An online job fraud scheme involves misleading people who require a job by promising thema better job with higher wages while giving them false hope. On March, 2022, the Reserve Bank of India (RBI) alerted people not to fall prey to job scams. By this, the RBI has explained the way in which online job fraud is perpetrated, as well as precautions the common man should take when applying for any job opportunity, whether in India or outside India.

Online Sextortion- In this type of fact the act of online sextortion occurs when the cybercriminal threatens any individual to publish sensitive and private material on an electronic medium. These criminals threaten in order to get sexual image, sexual favour or money from such individuals.

The act of Phishing- In this type of activity Fraud involving phishing is when an email appears to be from a legitimate source but contains a malicious attachment that is designed to steal personal information from the user such as their ID, IPIN, Card number, expiration date, CVV, etc. and then selling the information on the dark web.

A Vishing in this type of activity the person or victims' confidential information is stolen by using their phones. Cybercriminals use sophisticated social engineering tactics to get victims to divulge private information and access personal accounts. In the same way as phishing and smishing, vishing convincingly fools victims into thinking that they are being polite by responding to the call. Callers can often pretend that they are from the government, tax department, police department victims bank.

Smashing- This kind of attack the name suggests, smishing is a fraud that uses text messages via mobile phones to trick its victims into calling a fake phone number, visiting a fraudulent website or downloading malicious software that resides on victims computer.

Salami attacks- This kind of crime is normally prevalent in the financial institutions.

Denial of Service Attack- The Computer of the victim is flooded with more request than it can handle which cause it to crash.

Virus/worm attacks- Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. Love bug virus.

Logic bombs: This is a event depend programs. This implies these programs are created to do something only when a certain event (known as a trigger event)

Trojan attacks/Trojan Horse- This term is originated in the word 'Trojan horse'. In the software field. This means Unauthorised programme,

Internet Time thefts- Generally in this type of thefts Internet surfing hours of the victim are used by another person. This is done by gaining access to the login ID and the password.

Web jacking – This Concepts is transmitted from hi jacking. In these kinds of offences, the hacker gains access and control over the web site of another.

Data diddling attacks- This type of offence involves altering raw data just before a computer processer it and then changing it back after the processing is completed.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

Syber Law in India:

CYBER LAW Cyber Laws are incorporated in order to take control over crimes committed through the Internet or the cyberspace or through use of computer resources. Description of the lawful issues that are related to the use of communication of computer technology can be termedas Cyber Law.

The Information Technology law of India, 2000: According to Wikipedia "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), itwas 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.

Following are the Statutory provisions under IT Act, 2000:

1. Section 65. Temping with the computers source documents-Punishment: Any person who involves in such crimes could be sentenced up to 3 years imprisonment or with a fine of Rs 3 lakhs, or with both.
2. Section 66-Hacking with computer system, data alteration etc- Punishment: Any person who involves such crimes could be sentenced up to 3 years imprisonment, or with a fine that may extend unto 3lakhs rupees, or both.
3. Section 66A- Sending offensive messages through any communication services-Punishment: Any individual found to commit such crimes under this section could he sentenced up to 2 years of imprisonment along with a fine.
4. Section 66B- Receiving stolen computer's resources of communication devices dishonestly Punishment: Any person who involves insuch crimes could be sentenced either description for a term that may extend up to 2 years of imprisonment or with a fine of rupee 2 lakh or both.
5. Section 66C-Identify theft Using of one's digital or electronic signature of one's password or any other unique identification of any person is a crime. - Punishment: Arny person who involve in such crimes could be sentenced either with a description for a term which may extend up to 2 years of imprisonment along with a fine that may extend up to rupee2lakhs.
6. Section 66D- Cheating by personation by the use of computer's resources- Punishment- sentencedeither with a description for a term that may extend up to 3 years of imprisonment along with a fine that may extend up to rupee 2 lakh.
7. Section 66E- Privacy or violation Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas of private parts of any individual without his/her consent, that violets the privacy of the individual shall be shall he sentenced to 3 years of imprisonment or with a fine not exceedingly 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-Punishment: Whoever conspiresor commits such cybercrime or cyber terrorism shall be sentenced to life time imprisonment.
9 Section 67- Transmitting or publishing obscene materials in electronic farm- Punishment imprisonment 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 thatmay extend upto ten years along with a fine that may perhaps extend to two lakh rupees.
10. Section 67A- Transmitting or publishing of materials that contains sexually explicit contents, acts ete in electronics form- Punishment- Imprisonment for a term which may extend upto 5 years or imprisonment along with a fine that could extend to ten 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 upto7 years of imprisonment along with a fine that may extend upto 20 lakh rupees.
11. Section 67B- Transmitting or publishing of materials that depicts children in sexually explicit act etc inelectronics form-Punishment- Imprisonment for a term which may extend to 5 years of imprisonment with a fine that could extend to rupees ten 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 yoursalong with a fine that could extend to rupees 10 lakhs.
12. Section 67C- Retention and preservation of information by intermediaries I-Punishment: Whoever commits such crimes shall be sentenced for a period that may extend upto 3 years of imprisonment and also liable to fine.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, March 2024

II. CONCLUSION

Cybercrime in the latest and perhaps the most specialized and dynamic field in cyber laws. Some of the Cyber Crimes like network Intrusion are difficult to detect and investigation even though most of crimes against individual like cyber stalking cyber defamation, cyber pornography can be detected and investigated through following steps:

After receiving such types of mail:

- Give command to computer to show full header of mail.
- In full header find out the IP number and time of delivery of number and this IP number always different for every mail. From this IP number we can know who was the Internet service provider for that system from which the mail had come.
- To know about Internet service provider from IP number take the service of search engine like nic.com, macffvisualroute.com, apnic.com, arin.com.
- After opening the website of any of above-mentioned search engine, feed the IP number and after some time name of ISP can be obtained.
- After getting the name of ISP we can get the information about the sender from the ISP by giving them the IP number, date and time of sender.ISP will provide the address and phone number of the system, which was used to send the mail with bad intention.

REFERENCES

[1]. http;//www.statistia.com/statistics/ 267112/total-damage-caused-by-by-cyber-crime-in-the-
[2]. en.wikipedia.ong/wiki/ Phishing
[3]. www.tigway org/action tools/ projects downlond 5926.doc
[4]. https;// www.tutorialspoint.com/information security cyberlaws/introduction.hmt
[5]. https:// www.slideshare.net/bhuradwajchetan/anintroduction-to-cyber-law-it-act-2000-india
[6]. www.academia.edu/7781826/IMPACT OF SOCI AL MEDIA ON SOCIETY and CYBER
[7]. https://berstime.org .za/definition
[8]. https:// vikaspedia.in education Digital 20Litery inf formation-security/cyber-laws
[9]. htpps://www.ljarcise.com does papers Volume 33 Maj 2013/V315-0374.pdf
[10]. htpps:// searchroecurity techtarget.com.defined sporting