Ilkogretim Online - Elementary Education Online, 2021; Vol 20 (Issue 3): pp.3061-3068
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.03.316

An Overview Of India's Cybercrime And Cyberlaws

Ali Akhtar[1] , Ashutosh Singh[1] and Animesh Rishi[2]

[1]Institute of Legal Studies and Research, Mangalayatan University, Aligarh, UP.

[2]Faculty of Law, Usha Martin University, Ranchi, Jharkhand.

E-mail: ali.akhtar@mangalayatan.edu.in

Abstract: As is common knowledge, we live in an age where nearly everything is done online, from everyday shopping to major financial transactions. From any location, anyone can use the internet's resources because it is considered a global stage by many. There are a few persons that use the internet technology for illegal purposes, such as gaining unauthorised access to another's network or perpetrating hoaxes. The phrase cyber crime refers to these criminal behaviours or offences related to the internet. "Cyber Law" is a concept coined to deter and/or punish online crimes. We can refer to cyber law as the component of the legal system that deals with Internet, cyberspace, and legal difficulties. It encompasses a wide range of themes, including freedom of expression, Internet access and use, and online security or privacy. It is referred to as the web's law.

Key Words: Information Technology, Internet, Cyber-crime, Cyberspace, Cyber law, , Punish, Cyber Law & IT Law.

Introduction:

The government of the relevant country and state has established a legislation that allows for computer and cyber crimes. Crime and other offensive conduct such as computer and mobile crime, as well as IT crime can all be classified as Cyber Crime. Cyber Law is a set of rules and procedures that can be applied to a wide range of electronic crimes and offences [1]. Many individuals are still unaware about Cyber Crime and how to prevent it. The Government or constitutional entity or division of the concerned country or territory has essentially approved of the country's or territory's Cyber Law [2]. The number of instances is increasing daily, and the scope of Cyber Crime is expanding at an accelerating rate. As a general rule, cyber law comprises all laws relating to cybercrime, electronic crime, electronic signature & intellectual property crime, data security, information assurance, and so on There are various approaches to reduce cybercrime and cyber-related issues, which are briefly discussed in this paper. People aren't aware of the dangers of cybercrime, thus they don't take many safeguards [3].

Information technology has a profound impact on everyone's life. The internet and computer-based devices are utilised to make life easier and faster. As technology becomes more widely used, so does crime, which is on the rise as well. The term "cyber crime" encompasses all crimes involving computer networks. Criminals are increasingly attempting several attacks around the world in an effort to commit cybercrime. The culprits are well-educated and highly skilled technologists. For example, stealing money from a victim's bank account or accessing pornographic material are all examples of cybercrimes. There is a need to adopt some laws and regulations governing cyberspace called as Cyber Law in order to combat these crimes [4].

The Information Technology Act of 2000 has a number of provisions aimed at preventing and punishing cyber crimes. The cyber criminals who break the law are dealt with harshly. People who live outside of India are likewise subject to these regulations. The protection of cyberspace is a worldwide concern that necessitates international cooperation. Protecting computer resources and information from unauthorised use or disclosure is part of the process of implementing anti-virus software. People who work with computer networks must have a good knowledge of cyber law in order to create a safe and secure world in cyberspace.

Cyber Crime:

"Cyber Crime" was coined by Sussman and Heuston in 1995. It is impossible to define cybercrime in a single sentence; instead, it should be viewed as a series of actions or behaviours [5]. A substantial offence object that damages computer data or systems is the basis for these acts of terrorism. A digital device or information system can be used as a tool, target, or both in these crimes. Electronic crimes, computer-related crimes, e-crime, high-tech crimes, information age crimes, and so on are other terms for cybercrime.

To put it simply, "Cyber Crime" refers to criminal activity carried out via computer networks or electronic communications. Computer and network crimes are the most common sorts of criminal activity. There has been a rise in cybercrime activity as a result of the advent of the internet, as criminals no longer need to be present in order to perform their crimes via the internet. Cybercrime is rare in that the victim and the perpetrator may never meet face-to-face. In order to avoid detection and prosecution, cybercriminals typically choose to operate from nations with weak or nonexistent cybercrime legislation [6][9]. In the minds of many, cyber crimes can only be perpetrated on the internet or in cyberspace. According to a recent study, cybercrime can be performed even if the perpetrator is not present in the cyberspace at the time. As an illustration, consider the topic of software privacy.

The first known cyber crime occurred in 1820. Charles Babbage's analytical engine is regarded as the beginning of modern computers, despite the fact that computers have been around since 3500 BC in Japan, China, and India. The loom was invented in France in 1820

by Joseph-Marie Jacquard, a textile maker. In the weaving of unique textiles or materials, this mechanism allowed for a sequence of processes that were continuous. Jacquard's workers feared that the new technology would put their jobs at risk, and they decided to sabotage the company in order to prevent it from using the new method of production in the future.

From Morris Worm to ransomware, cybercrime has progressed. India is one of several countries trying to curb these attacks and crimes, yet they are evolving and impacting our country.

Classifications of Cyber Crime:

There are four main categories of cyber crime. These are the names of them:

a)This includes crimes perpetrated by cyber criminals against an individual or a human being. Here are a few examples of online crimes committed against specific individuals:

An email header spoof is a fabrication in the form of a fake email address. As a result, the communication looks to have been sent by someone or somewhere other than the true or actual originator of the message Spam and phishing efforts often utilise this strategy because individuals are more likely to open an email that appears to have been sent from a trusted source.

The term spam refers to the practise of sending out unwanted emails, which is also known as junk mail. It's an unwelcome email that's been sent to a large number of people. Most email users today confront the challenge of dealing with spam, which was first popularised in the mid-1990s. Spam bots, which are automated programmes that scour the internet for email addresses, collect the recipients' addresses. In order to compile email distribution lists, spammers rely on spam bots. Spammers often send an email to millions of recipients in the hopes of gaining a few responses.

Cyber defamation: The injury done to a person's reputation in the eyes of others through the internet is called "cyber defamation." Making a defamatory statement is a way to harm someone's reputation.

Using IRC servers, people from all over the world can talk with one other in a single room, which is sometimes referred to as a "channel." Cyber criminals primarily use it for meetings. This word is used by hackers to describe their methods. To entice little toddlers, paedophiles utilise it. It is common for IRC criminals to gain the trust of their victims, then harass them sexually, blackmail them for ransom, and threaten to post their victims' nude photos or videos online if they don't pay up. One or two of them are predators who prey on children for their own gain. IRC is used by a few people who advertise bogus jobs and lottery prizes and make money.

Fraudsters try to steal personal information, such as passwords, by pretending to be trustworthy individuals or organisations via multiple communication channels or by email. Net extortion, hacking, public indecency, trafficking, distribution, posting, credit card fraud, malicious code, and other forms of cybercrime that target individuals are also on the list. There is no way to overstate the potential harm that such a deterioration could cause to a single individual [7].

b) Vandalism of computer systems, intellectual property theft, and online threats are all examples of cybercrime against property. Infringement on a third party's intellectual property rights includes:

It is possible to define "software piracy" as the act of copying software without permission.

Infringement of a person's or organization's copyright is what is meant by "copyright infringement." It can also be referred to as the unauthorised use of copyrighted materials, such as music, software, and text.

Unauthorized use of a service mark or brand constitutes trademark infringement.

c) The following are examples of cybercrimes committed against an organisation:

Data tampering or erasing without permission.

Unauthorized reading or copying of confidential information, although the data are not being altered or erased.

As part of a DOS assault, the attacker floods target servers, systems, or networks with traffic so that the victim's resources are overwhelmed and users are unable to access them.

If an email address receives an overwhelming quantity of emails, it is known as "email bombing," which is an example of a sort of Net Abuse known as "email spamming."

Salami slicing is another term for the Salami attack. Customers' bank account and credit card numbers, among other personal information, are stolen via an online database assault. Over a period of time, the attacker steals a small sum from each account. Because the victims are unaware of the slicing, no complaints can be filed, and the hackers can therefore remain undetected. Other types of cyber-attacks against organisations include logic bombs, Torjan horses, and data tampering, among others [8].

d) The following are examples of cybercrime committed against society: • Forgery: Forgery refers to the creation of a fraudulent document, signature, cash, revenue stamp, or any other similar piece of counterfeit material.

It's called "Web jacking" since the term "hi jacking" was used to describe it. When the victim clicks on a link on the attacker's bogus website, a new page pops up asking them to click on another link. Clicking on a link that appears to be authentic redirects the victim to a phoney

website. These kinds of assaults are used to gain access to or control another person's site. Additionally, the attacker may alter the victim's website.

India's cybercrime situation: a few case studies

NSP's Bank Case An employee of a bank became engaged to a manager trainee. A lot of their correspondence took place over email, which they did on the machines provided by the corporation. Eventually, the couple divorced, and the young lady started using fictitious email addresses like "Indian bar associations" to contact the young man's international clientele. This was all done on the computer at the bank. The bank was taken to court by the boy's firm after losing a large number of customers. In this case, the bank was held responsible for the emails that were sent through the bank's network.

Case of Bazee.com When the CEO of Bazee.com was arrested in December 2004 for selling a CD containing obscene information on the website, the CD was also sold out in the Delhi market simultaneously. The CEO was arrested by the Delhi Police, who then turned to the Mumbai Police, who were able to discharge him on bail.

The House of Representatives Attacks the Case This case was handled by the Hyderabad Bureau of Police Research and Development. One of the terrorists responsible for the attack on Parliament had a laptop that was found. BPRD's Computer Forensics Division received the laptop that belonged to the two terrorists who were gunned down on December 13th, 2001, while the Parliament was under siege. It was discovered that the two terrorists used the laptop to make a fake Ministry of Home sticker, which they attached to their ambassador car in order to gain admission into Parliament, as well as a false Indian ID card that one of them was carrying with an Indian flag and seal. The three lion symbols were meticulously scanned, and a seal with a Jammu and Kashmir address was handcrafted from scratch. However, a thorough investigation revealed that everything had been fabricated on a laptop.

The Tax Case in Andhra Pradesh The proprietor of a plastics company in Andhra Pradesh was detained and Rs. 22 was seized from his home by the Vigilance Department.. He was asked to provide proof of the money's whereabouts. However, following careful examination of the 6,000 vouchers and the contents of the suspect's computers, it was discovered that every one of them was made after the raids were done. False and computerised vouchers were used to show sales records and save tax in the suspect's five businesses that were hidden under the umbrella of a single company. That's what happened, and it exposed the shady practises of a businessman from the state who had computers in his possession.

SONY.SAMBANDH.COM CASE The first cybercrime conviction was made in India. For example, Sony India Private Limited has filed a complaint alleging that their NRI-targeting website www.sony-sambandh.com has violated the Indian laws. NRIs can pay for Sony products online and then send them to friends and family in India. Delivery of the products will be made on behalf of the company. In May of 2002, someone used Barbara Campa's e-

mail address to order a Sony colour television and a cordless headphone from the company's website. For payment, she provided her credit card details and requested that the product be sent to Arif Azim in Noida. As a result, the credit card company cleared the payment and processed the transaction. The items were provided to Arif Azim by the company after they had completed the necessary due diligence and inspection procedures. As soon as the package was delivered to Arif Azim, a digital photograph was taken to show that he had accepted the delivery. After one and a half months, the credit card company notified the company that the purchase had been made without authorization because the true owner had denied making it. The corporation had submitted a complaint for internet cheating at the CBI that lodged a case under the Section 418, Section 419 and Section 420 of the IPC (Indian Penal Code). After an investigation, Arif Azim was taken into custody. Investigations discovered that Arif Azim, when functioning at a call centre in Noida did acquire access to the number of the credit card of an American national which he exploited on the company's site. In addition to the cordless phone, the CBI recovered a colour television. The CBI had enough evidence to convict the accused in this case, so he admitted his guilt. The court found Arif Azim guilty of violating Sections 418, 419, and 420 of the Indian Penal Code, making him the first person to be found guilty of a cybercrime. Because the defendant was only 24 years old and a first-time offender, the court decided to take a more lenient stance. Thus, the court sentenced the defendant to one year of probation.

India's Cyber Laws:

Act on Information Technology (IT) (2000 Sections)

Section 65- Toying with the computer's underlying data files. A computer, computer programme, computer system, or computer network whose source code has been destroyed, concealed, or altered with malice aforethought.

Punishment: Anyone found guilty of such offences faces a penalty of up to three years in prison, a fine of up to Rs.2 lakh, or a combination of the two.

Section 66- Data tampering and hacking, for example The person or persons who intend to inflict harm to a computer system, whether it's a public one or an individual's, or who attempt to gain unauthorised access to a computer system. Hacking is the act of reducing something's usefulness or worth or harming it adversely in any way.

Punishment: A person who commits such offences could face up to three years in prison or a fine of up to 2 lakh rupees, or both, if convicted.

Section 66A- Sending obscene or otherwise offensive messages via any form of electronic communication. The use of any kind of communication service to send any kind of abusive or threatening content. Information that is fabricated, deceitful, malicious, or ill-intentioned and sent with the objective of annoyance, inconvenience, danger, insult and obstruction.

Messages transmitted with the intention of causing distress or confusion or deceiving the recipient as to their origin.

Punishment: A person convicted of a crime under this section could face up to three years in prison and a fine.

Section 66B- Computer resources or communication equipment that have been obtained dishonestly Stolen computers, computers' resources or communication devices can be found in the possession of anyone who knows or has cause to suspect they are stolen.

Punishment: Anyone found guilty of such offences faces a prison sentence of up to three years or a fine of Rs. 1 lakh, or a combination of the two.

Section 66C- Theft of a person's identity It is a criminal to use someone else's digital signature, password, or other unique identifier.

Punishment: Anyone found guilty of such offences faces a penalty of up to three years in prison and a fine of up to one lakh rupees (about $15,000).

Section 66D- cheating through the exploitation of a computer's resources by assuming another person's identity A person who tries to deceive someone by impersonating them through any communication device or computer's resources can face up to three years in prison and a fine of up to one million rupees.

Section 66E- A breach of confidentiality or a violation of privacy It is against the law for anybody to publish photos of an individual without their permission, or to capture images of an individual's private areas or private parts without permission, to be sentenced to 3 years in prison or a fine not exceeding 2 lakh rupees, or both.

Conclusions:

In recent years, numerous cybercrimes have been facilitated by the growth and dissemination of new technologies. In today's world, cybercrime poses a serious threat to humanity. A country's social, cultural, and security aspects all depend on its ability to combat cybercrime. To combat cybercrime, the Indian government created the IT Act, 2000. Among the many amendments made by the law are those to the Indian Penal Code (IPC) (1860), the Indian Evidence Act (IEA) (1872) (Indian Evidence), the Banker's Books Evidence Act (1891) (Banker's Books Evidence Act, 1891), and the Reserve Bank of India Act (1934). Cybercrime can originate from anywhere in the globe, crossing national borders via the internet, complicating investigations and prosecutions in both technological and legal ways. All nations must work together in an international effort to combat cyber crime. Our primary goal in writing this paper is to educate the general public about the dangers of cybercrime. "A brief research on Online Crime and Cyber Law's of India" concludes by saying that cyber crimes are never acknowledged. Anyone who has been the victim of a cyberattack should

come forward and file a report with the local police department. If the perpetrators are not held accountable, they will continue to commit crimes.

References:

1. Cohen, Eli B. and Nycz Malgorzata (2006). Learning Objects and E-Learning: an Informing Science Perspective. Interdisciplinary Journal of Knowledge and Learning Objects Volume 2, 2006

2. Seema Vijay Rane & Pankaj Anil Choudhary, April 2012-September 2012, "Cyber Crime and Cyber Law in India", Cyber Times International Journal of Technology and Management, Vol. 5 Issue 2

3. Michael Buckland and Ziming liu (1995).History of information science. Annual Review of Information Science and Technology vol. 30: 385-416. 5. P.K. Paul, " Information Scientist: Roles and Values w

4. Sheri R.K. & Chhabru S.T.N 2002, "Cyber Crime", New Delhi, Pentagon Press

5. P.K. Paul, " Information Scientist: Roles and Values with special Reference to their Appropriate Academic Programme and its availability in India:" International Journal of Information Dissemination and Technology, Vol. 2, No. 4, October-December-2012, Page-245-248, ISSN-2229-5984

6. S. Sai Sushanth, "Cyber Law: Various Aspects of Cyber Legal System", Cyber Times International Journal of Technology and Management.

7. White, H.D., & McCain, K.W. (1997). Visualization of literatures. Annual Review of Information Science and Technology, 32, 99–168

8. Ryder D. Rodney 2007, "Guide to Cyber Laws", Nagpur Wadhawa and Company

9. Harish Chander 2012, "Cyber Laws and IT Protection", PHI Learning