Cyber Crime in India: An Overview

[1]Mr. Pravej Alam, [2]Mrs. Richa Tiwari

Research Scholor
Nims University, Rajasthan (Jaipur

Abstract: As we all know, we live in an era where most things are done over the internet, from online dealing to online transactions. Because the internet is considered a global stage, anyone from anywhere can access its resources. Few people have used internet technology for criminal purposes such as unauthorized It is broad in scope, encompassing many subtopics such as free expression, access to and use of the Internet, and online security or privacy. It is commonly referred to as the law of the web. access to other people's networks, scams, and so on. Cybercrime refers to criminal activities or offenses/crimes committed via the internet. The term "Cyber Law" was coined in order to deter or punish cyber criminals. Cyber law can be defined as the part of the legal system that deals with the Internet, cyberspace, and legal issues.

Keywords: -Internet, Unauthorized access, Cybercrime, Cyber law, Cyberspace, Punishment, Network are some key words.

1. INTRODUCTION

In universal, the term 'Cyber Law' refers to all legal and governing parts of the Internet. It refers to anything concerned with, related to, or rising from any legal aspects or issues. Cyber law applies to any activity of netizens and others in cyberspace. More definitely, cyber law is defined as the law that governs the use of computers and the Internet. Its efforts on a variety of state and federal statutory, decisional, and administrative laws arising from Internet use.

In general, the term 'Cyber Law' refers to all legal and governing aspects of the Internet. It means anything concerned with, related to, or arising from any legal aspects or issues about any netizen's activity.

The term cybercrime may be judicially interpreted in some Indian dispute settlement, but it is not described in any act or law passed by the Indian Parliaments. Cybercrime is an unexpected act with its origins in the web.in the modern increasing world reliance on computers. The use of computers and other affiliated digital in daily life is rising rapidly and has become a desire that facilitates user convenience. It is an infinite and immeasurable medium. Whatever good the internet does for us, it also has a negative side likely Cyberstalking, cyberterrorism, e-mail spoofing, e-mail bombing, cyber pornography, cyberdefamation, and other newly emerging Cybercrimes are examples. Some formal crimes may be classified as Cybercrimes if they are committed online.[1]

1.1 Definition of Cyber Crime

The Indian Legislature does not define Cybercrime in any statute; even the Law on Information Technology of 2000, which deals with Cybercrime, does not define the term. However, in general, Cybercrime refers to any criminal activity carried out through or with the assistance of the internet or computers.

According to [2] Dr.Debarati Halder and Dr. K. Jaishankar[3] define cybercrimes as:

"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".

We do not have any precise definition of Cybercrime; however, following is the general definitions of term Cybercrime: The oxford Dictionary defined the term cybercrime as "Criminal activities carried out by means of computers or the Internet."[4]

"Cybercrime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime"[5]

"Cybercrime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them"[6]

1.2 Nature and Scope of Cyber Crime

Criminal activity is a social concept. We will never be able to live in a society without Cybercrime, no matter how hard we try. In reality, when we are unable to reduce crime rates to a desirable level in the How would it be possible to reduce the same in the digital world, given that it is fairly more unreal, eternal, and legally less controllable? However, the nature, scope, and definition of crime in a given society change over time. A crime-free society is a myth, and crime cannot be isolated from society. Thus, the nature of crime is determined by the character of a humanity.

[1] Prof. R.K.Chaubey, "An Introduction to Cyber Crime and Cyber law", Kamal Law House, 2012

[2] Professor of Law, Parul Institute of Law, Parul University, Vadodara, Gujarat, India

[3] Professor K. Jaishankar Ph.D.Founder | Principal Director & Professor of Criminology & Crime Sciences at International Institute of Crime & Security Sciences (IICSS) | Father of Cyber Criminology | 16 of Top 25 World's Influential Criminologists |

[4] http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 4th January, 2023)

[5] http://www.naavi.org/pati/pati_cybercrimes_dec03.htm (Accessed on 4th January, 2023)

[6] http://cybercrime.org.za/definition (Accessed on 4th January, 2023)

The complex nature of society impacts the difficulty of crime that emerge around it. Explaining crime in a society needs confirm all of the factors that influence and contribute to crime. The socioeconomic and political structures of society must understand crime and the remedial measures available to address it. When trying to study the nature and scope of a crime, the machinery's preventive and corrective measures to control crime and delinquent behavior and conduct are also taken into consideration.

Digital innovation has introduced new economic and political challenges for society, and instead of helping the state in managing the problem, it has created a new complex situation that is difficult to understand and even more difficult to apply current law to face. The state system is not furnished with enough sources and understanding to manage the modern crime.

In the last three to four eras, computers have transformed modern society in ways that no one could have predicted. It has not only made life more convenient, but it has also greatly aided in the social, economic, and cultural integration of different parts of the world. Computer technology has enabled access to all corners of the globe while sitting in a single room. Time and space barriers have been broken down by modern technology. However, with the amazing benefits of having computers today, a regulatory issue has emerged in the legal system.

As a result, the global scope of cybercrime makes it difficult to manage and combat. The advancement of digital technology has granted us with many advantages in dealing with future problems and growing at a rapid rate, but it has also provided opportunities for lawbreakers to commit their crimes with little chance of detection. The cyberspace has been a boon to society's delinquent acts. The concept of Cybercrime has gained momentum, and we are facing a serious risk from its impact on global society. Because of our increasing dependence on technology, human society is growing more sensitive to cybercrime.

As a result, the threat of cyber terrorism poses a serious challenge to the world and its institutions. Terrorist organizations use technology to spread hatred among people, as well as to recruit armed groups and train them using teaching tools. They are also launching online sites that tell them how to use weapons and make bombs, among other things.[7]

1.3 Characteristics of Cyber Crime

Cybercrime is not the same as traditional crime. In addition, as Internet technology has advanced, this crime has received more serious and unfettered attention than traditional crime. As a result, it is necessary to investigate the unique characteristics of Cybercrime.

- **People with specialized knowledge: -** Cybercrimes can only be committed through technology, so to commit such a crime, one must be very skilled in the internet, computers, and the internet. People who commit Cybercrime are well educated and have a thorough understanding of how the internet works, making it difficult for police to catch the perpetrators**.**
- **Geographical challenges: -** Geographic boundaries vanish in cyberspace. A cyber-criminal can commit a crime in another part of the world while sitting in one part of the world. For instance, a hacker in India could compromise a system in the United States.
- **Virtual World: -** A cyber-crimes happen in cyberspace, but the criminal committing the crime is physically beyond the cyberspace. Every action taken by the criminal while committing the crime takes place in the virtual world.
- **Collection of Evidence: -** Due to the nature of cybercrime, gathering evidence and proving it in court is extremely difficult. While committing cybercrime, the criminal invokes the statutory authority of many countries while sitting somewhere safe where he is untraceable.
- **Magnitude of crime unimaginable: -** Cybercrime has the potential to cause bodily injury death and injury on an unprecedented level. Cyber terrorism, cyber pornography, and other crimes have a broad reach and can quickly destroy websites and steal company data.

2.Classifications of Cyber Crime

1.1 Cyber Terrorism

Cyber terrorism is the use of a computer and the web to commit violent acts that cause death. This could include a variety of activities carried out by software or hardware to damage the life of citizens. In general, cyber terrorism is defined as a terrorist act committed using cyberspace or computer resources. Cyber terrorism is the use of a computer and the internet to commit violent acts that result in death. This could include a variety of activities carried out by software or hardware to endanger the lives of citizens. In general, cyber terrorism is defined as a terrorist act committed to use cyberspace or computer resources.

2.2 Cyber Extortion

When a website, e-mail server, or system software is applied to or attacked with repetitive refusal of system or other attacks by computer attackers, cyber extortion occurs. These hackers demand large sums of money in exchange for assurances that the attacks will be prevented and that they will be kept safe.

3.3 Internet Fraud

Internet fraud is a type of fraud or deception that uses the Internet to deceive victims for money or property. It may include hiding evidence or providing misleading data. Internet fraud is not a single, distinct crime, but rather a collection of illegal and illicit process performed out in cyberspace.

4.4 Cyber Stalking

This is a type of online harassment in which the victim is bombarded with online messages and emails. In this case, the stalkers know their victims and, instead of stalking them in person, they stalk them online. If they notice that cyber stalking is not making a positive impact, they will begin offline stalking in relation to cyber stalking in attempt to make the victims' lives even more uncomfortable.[8]

[7] J.W.C. Turner, Kenney's Outlines of criminal law (19th Edition University Press, Cambridge 1966) 17. also at Talat Fatima, Cyber Crime (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

[8] https://www.geeksforgeeks.org/cyber-crime/(Accessed on 4th February, 2023)

3 Cyber Crime in India an overview

3.1 HISTORY OF CYBER CRIME

The first instance of cybercrime was recorded in 1820.The first type of computer was found in Japan, China, and India around 3500 B.C., but Charles Babbage's analytical engine is considered to be the birth of modern computers. The loom was invented in France in 1820 by a textile manufacturer named Joseph-Marie Jacquard. This device enabled a continuous series of steps within the weaving of special fabrics or materials. As a result, Jacquard workers were extremely concerned that their livelihoods and traditional employment were under threat, and they preferred to sabotage in order to discourage Jacquard from using the new technology in the future.[9]Currently, a lot of individuals utilise the internet and conduct online transactions utilising a variety of apps like Paytm, Phone Pay, and Google Pay. Online hackers then use emails, phone calls, etc. to commit their crimes.

3.2 ACTS CONNECTED WITH CYBERCRIME IN INDIA

The Information Technology Act, 2000 and the Indian Penal Code, 1860 both apply to Cybercrimes in India. The Information Technology Act of 2000 is the law that addresses matters relating to online crime and internet trade. The Act was modified in 2008 to include a definition and punishment for cybercrime, nevertheless. Additionally, changes were made to the Reserve Bank of India Act and the Indian Penal Code 1860.[10]

3.3 CASE STUDIES CONCERNING CYBERCRIME

3.3.1 Bazee.com case (Avnish Bajaj vs State on 29 May, 2008)

Because a CD containing inappropriate information was being sold on the website in December 2004, the CEO of Bazee.com was detained. Additionally, Delhi markets were selling the CD.

Both the Mumbai Police and the Delhi Police acted. Later, bail was paid to free the CEO. The issue of how to distinguish between Internet Service Providers and Content Providers was raised as a result. It is the accused's responsibility to prove that he provided the service and not the content. Additionally, it raises several questions about how law enforcement should approach cybercrime cases.

3.3.2 The Bank NSP Case NSP (ASSOCIATES INDIA PVT LTD v. SYNDICATE BANK.11.03.2019)

The Bank NSP case, in which a management trainee from the bank was engaged to be married, is one of the most prominent cybercrime instances. Using the company computers, the pair exchanged a lot of emails. Following their breakup, the girl created phoney email accounts like "indianbarassociations" and started sending emails to the boy's international clientele. She carried out this task on the bank's computer. The boy's business lost a lot of customers and sued the bank. For emails sent via the bank's system, the bank was held accountable.

3.3.3 Cyber Attack on Cosmos Bank (August 2018,)

In a very audacious cyberattack in August 2018, the Cosmos Bank branch in Pune lost Rs 94 crores. The money was transferred to a Hong Kong bank by the thieves once they broke into the main server. Along with this, the hackers gained access to the ATM server in order to obtain information about numerous VISA and Rupay debit cards.

Because the switching system, which serves as the link between the centralised system and the payment gateway, was targeted, neither the bank nor the account holders were made aware of the transfer of funds.

A total of 14,000 transactions were made using 450 different cards across 28 different countries, according to a global case study on cybercrime. 400 cards were used for 2,800 transactions nationwide. This was the first malware attack of its sort to completely halt connection between the bank and the payment gateway.

3.3.4 Cyber Terrorism

This instance of cyberterrorism was the first to be implemented after the Information Technology Act underwent revisions in Mumbai. At 10:44 on Monday morning, a threatening email was sent to the BSE and NSE. The culprit has been detained as a result of joint investigation efforts by the MRA Marg police department and the Cyber Crime Investigation Cell (CCIC) into a cybercrime case. Bihar's Patna was the location of the IP address. Two contact numbers were uncovered after searching for any personal information, and they belonged to a Patna-based company that made picture frames.[11]

3.3.5 Shreya Singhal Vs UOI AIR 2015 SC 1523

The two ladies were detained under Section 66A of the IT Act for allegedly posting offensive remarks on Facebook about the full closure of Mumbai after the death of a political leader. Section 66A of the IT Act specifies that anybody who transmits material that is offensive, false, or causes discomfort, danger, irritation, insult, hostility, harm, or ill will via the use of a computer network or communication faces imprisonment. The ladies filed a petition contesting the validity of Section 66A of the IT Act, claiming that it violates their right to free speech and expression.

The legality of Section 66A of the IT Act was questioned in the Supreme Court. Decision While rendering the judgement court highlighted three ideas and they were debate, advocacy, and incitement. The court held that simple debate or even endorsement of a subject, no matter how unpopular, is at the essence of free speech and expression. The court ruled that Section 66A is unclear, violates the right to free expression, and includes harmless speech within its scope. It repealed an arbitrary clause in the Information Technology Act of 2000 and defended people' basic right to free expression in India. It was of the opinion that even if Section 66A

[9]] https://www.ijarcsse.com/docs/papers/Volume_3/5_ May2013/V3I5-0374.pdf

[10] https://blog.ipleaders.in/cyber-crime-laws-in-india/(Accessed on 14th February, 2023)

[11] https://www.cyberralegalservices.com//(Accessed on 14th February, 2023)

is invalidated, sections in the Indian Penal Code, 1860 would continue to apply forbidding racist speech, any communication that offends a woman's modesty, or speech aiming at fostering enmity, abusive language, false imprisonment, racism, and so on.

4.Conclusion

With the growth of technology, disturbing elements are developing on the dark web that is alarming. The Internet has become a weapon of bad activities that are used by intelligent minds for bad intentions and usually for financial benefit. Thus, at this stage in time, cyber laws enter into the scene and are important for every individual. As a result, that cyberspace is an extremely difficult environment to deal with, certain actions are classed as grey activities that cannot be managed by legislation**.**

To keep up with the rising dependency of people on technology, cyber laws in India and throughout the world must be constantly updated and revised. As a result of the epidemic, there has also been a large growth in the number of remote employees, which has raised the demand for application security. Legislators must take additional steps to stay ahead of imposters and take action against them as soon as they appear. It can be stopped if legislature, service providers, Banks, Shopping websites and other intercessors act together. However, it is ultimately up to users to take part in the battle against cybercrime. The only way for online safety and resilience to flourish is for these stakeholders' activities to be scrutinised to ensure they remain within the bounds of cyberspace law.[12]

[12] https://blog.ipleaders.in/cyber-crime-laws-in-india/(Accessed on 15th February, 2023)