CYBERCRIME

Pallavi Kumari*

"Neither the internet nor Cyberspace will ever be a secure haven for people that attempt this type of cybercrime. The Secret Service in conjunction with our enforcement partners will hunt you down, the keystroke to the keystroke." – Brian Marr

ABSTRACT

The Internet is a crucial part of contemporary life. Technology improvements have made the internet more pervasive in our lives than we could have ever imagined. Cybersecurity is essential in the realm of information technology. Information is being disseminated more widely every day as new social media sites pop up and use millions of bytes of data per second throughout the world. These files include extremely private information, including trade secrets, personal data, and security issues. Information security is one of the biggest problems in contemporary society. The word "cybercrime" is used to characterise these illegal activities or the crime/offence related to the internet. When referring to actions done to prevent or punish online crimes, the term "Cyber Law" was first used.

INTRODUCTION

Cybercrime is the greatest sector of the world economy in terms of criminal growth. Any illegal activity involving a computer, networked device, or network is referred to as cybercrime. Cybercriminals may commit some crimes in order to profit from their actions; they may also harm or disable computers directly; still, others may use computers or networks to spread viruses, unlawful data, offensive photos, or other content. The potential for illegal activity has increased along with the enormous growth of the Internet. The growing global usage of the Internet has led to an increase in computer crimes, including extortion, child pornography, money laundering, fraud, software piracy, and corporate espionage, to name a few. Law enforcement officials are dissatisfied with Congress' failure to update cybercrime legislation with the

In a nutshell, "Cyber Crime" is the term used to describe offences or crimes perpetrated via the use of electronic communications or information systems. These offences are

*LAW GRADUATE.

fundamentally illegal network or computer-related behaviours. Due to the advent of the internet, it is no longer essential for a criminal to be physically present in order to commit a crime, which has led to an increase in the number of cybercrime operations.

The weird thing about cybercrime is the possibility of never meeting the culprit or victim in person. Cybercriminals typically prefer to operate out of nations with lenient or non-existent cybercrime legislation to reduce their chances of being detected and convicted.

CYBER CRIME AND CYBER LAW

A "Cyber Crime" is defined as any illegal activity or other infringement using electronic communications, information systems, any kind of gadget, the Internet, or even more than one of these. The term "cyberlaw" refers to the legal issues connected to the use of communications technology, namely "cyberspace," which is the Internet. The challenge offered by online misbehaviour is combined with the established legal system that rules the real world in this attempt.

CLASSIFICATION of CYBER CRIME

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

CYBER CRIMES AGAINST INDIVIDUALS: crimes that are perpetrated against a person or a person by cyber offenders. Among the cyber crimes committed against persons:

Email spoofing: This trick pretends to be an email header. This shows that a different source than the legitimate one appears to have sent the message. Since people are more likely to read an email or other electronic message if they think it came from a trustworthy source, these tactics are commonly used in spam campaigns or phishing.

Spamming: Email spam is also known as junk email. Unwanted email mass messaging is what this is. The middle of the 1990s saw the widespread adoption of spam, and most email users today still battle with it. Recipients' email addresses are gathered by spam bots, which are automated programmes that scan the internet for email addresses. Spammers create email distribution lists using spam bots. In the hopes of receiving a few answers, spammers frequently send emails to millions of email accounts.

Cyber defamation: The word "cyberdefamation" refers to damage done to a person's reputation in the eyes of others via the internet. The purpose of making false remarks is to harm someone's reputation.

IRC Crime (Internet Relay Chat): In order to speak with one another, people from all over the world can gather on IRC servers in a place called a room. Essentially, it is used for gatherings by cyber criminals. There, hackers talk about their techniques. Paedophiles use it to lure young children.

A few reasons behind IRC Crime:

- When someone is being blackmailed for money, the criminal first tries to gain their trust before beginning to harass them sexually. If the victim refuses to pay the ransom, the criminal then threatens to post the victim's naughty pictures or videos online.
- Some people abuse children for their gain; they are known as paedophiles.
- Some people use IRC to advertise phoney jobs and occasionally bogus lotteries to make money.

Phishing: The perpetrators of these sorts of crimes or fraud use different communication channels or emails to pose as a reputable person or organisation in order to get information such as login passwords or account information. Credit card fraud, net extortion, hacking, indecent exposure, trafficking, distribution, uploading, and harmful code are a few more crimes performed against individuals online. A person could rarely suffer any further injury from such a malefaction.

CYBER CRIME AGAINST SOFTWARE: These crimes include internet threats, intellectual property offences (Copyright, patented, trademark, etc.), computer vandalism, and other types. Intellectual property offences consist of:

- **Software piracy:** Unauthorised software copying is what is meant by this term.
- **Copyright infringement:** This is the violation of someone's or an organization's copyright. It can also be summed up simply as the unauthorised use of copyright materials like music, software, text, etc.
- The unauthorised use of a service mark or trademark is known as trademark infringement.

CYBER CRIME AGAINST ORGANISATION: The following list of cybercrimes against organisations:

- Unauthorised deletion or alteration of data.
- Unauthorised access to private information by reading or copying that doesn't change or remove the data.
- When a server, system, or network is subjected to a denial-of-service assault, the attacker overwhelms the victim's resources and makes it difficult or impossible for users to utilise them.
- Email bombing: This type of online abuse comprises sending several emails to one address in an effort to clog the inbox, overwhelm the server that hosts the address, or both.
- Salami assault: Another name for a salami attack is salami slicing. In this assault, the criminals use an online database to acquire customer data, including bank and credit card information. The attacker gradually withdraws very little money from each account. Because the victims are unaware that they are being sliced in this attack, no complaints are raised, and the hackers remain undetected.

  Among other cybercrimes committed against companies, logic bombs, Trojan horses, and data manipulation are also common.

CYBER CRIME AGAINST SOCIETY: Cyber Crime against society includes:

- Forgery: This term refers to the creation of fake documents, signatures, money, revenue stamps, etc.
- Web jacking: This behaviour is derived from the word "hijacking." The link to the attacker's fake website appears when the victim clicks it, and a new page with the message opens, asking them to click another link. If the victim clicks on the link that seems legitimate, a fake website will be loaded instead. These sorts of offences are committed to get access to another person's property or to get inside and seize power. The information on the victim's website could have been changed by the attacker.

HISTORICAL BACKGROUND OF CYBER CRIMES.

In the 1870s, the advent of cybercrimes began when teenagers were first recognised for their phone calls. By the 1990s, the internet was viewed as an amazing medium with the quickest speed in human history and a growing reliance on technology. The first polymorphic virus

was launched in 1992, during the first cybercrime case. Yahoo v. Akash Arora[1] was the first cybercrime case in India. A permanent injunction was asked since the accused was using the domain name or trademark "yahooindia.com" when the case was heard in 1999.

Later, it was found that section 43 of the IT Act, 2000, bans accessing another person's email accounts without that person's consent in the case of Vinod Kaushik and others v. Malvika Joshi and others, 2013. In the end, crime rose with technological growth.

ROLE OF THE INDIAN LEGISLATURE

In response to the rise in cybercrimes, the Indian Parliament created the Information Technology Act in 2004. It was later updated in 2008. Additionally, the IT Act updated specific parts of the Indian Penal Code of 1860, the Banker's Book Evidence Act, and the Evidence Act of 1872 to match contemporary technology. The IT Act covers the offences and punishments under the Indian Penal Code of 1860 and other legislation; it does not, however, define cybercrime. Cyber laws are meant to offer legal recognition for all electronic transactions, accept digital signatures as acceptable for entering online contracts, acknowledge that banks and other organisations retain accounting records electronically, safeguard online privacy, and put an end to cybercrimes.

The amendment was passed in 2008[2], and it became operative in 2009 after receiving the president's approval. The fifth amendment act (amendment act) focused on information security, data privacy, defining cybercafés, creating digital signatures, defining reasonable security practises to be followed by corporations, redefining the role of intermediaries, identifying the Indian Computer Emergency Response Team, including some additional cybercrimes like child pornography and cyberterrorism, and authorising an Inspector to investigate cyber offences.

The law is divided into 30 chapters and 90 parts. The act begins with introductory provisions and definitions, Chapter II deals with digital signatures and electronic signatures, Chapter III deals with electronic governance, and the legal recognition of signatures and records, and Chapter IV deals with the attribution, acknowledgement, and dispatch of electronic records from Chapter I. Computer viruses, compute contamination, computer database, and source

[1] 1999 IIAD Delhi 229, 78 (1999) DLT 285
[2] Information Technology Amendment Act 2008 (IT Act 2008)

code are all defined in this section. Chapter XI deals with crimes that are not susceptible to bail.

The list of sections is expanded to include Sections 66A through 66F. The sections cover crimes such as using a communication service to send violent messages, lying to the recipient about the origin of such messages, dishonestly obtaining stolen computers or other communication devices, stealing electronic signatures or identities, such as by using another person's password or electronic signature, cheating by characterization using computer resources or a communication device, and publishing information about any person's location in public. It should also be highlighted that section 43 is a civil law provision that provides for damages and compensation as remedies. A person may be charged criminally and punished with a fine, a jail sentence, or both if they act with the intent to commit a crime, in accordance with Section

The term "hacking" was modified in Section 66-7 to "data theft," which made it clear that "hacking" is only done with the owner's consent and that "cracking" is prohibited. Email spoofing is defined in Section 66A as the act of sending emails or other electronic communications that are offensive with the goal to confuse or irritate the recipient regarding the real source of such messages. These violations carry a maximum three-year jail sentence or a fine. Under Section 66B, obtaining a stolen computer resource or piece of communication equipment dishonestly carries a three-year prison term, a fine of one lakh rupees, or both.

Section 66C: Possession of an electronic signature or identity theft, such as using someone else's password or electronic signature, are crimes that carry a three-year prison term, a one lakh rupee fine, or both.

The use of a computer or communication device to impersonate another person is prohibited under Section 66D and is subject to a fine of at least one lakh rupees or a sentence of up to three years in jail. Without the consent of the individual, any information or private content may not be published in accordance with Section 66E, which entails a three-year prison sentence or a two-lakh fine.

Paragraph 66F The purposeful attempt to compromise someone's rightful access to a computer resource or to breach or get unauthorised access to a computer resource with the intention of jeopardising the unity, integrity, security, or sovereignty of the nation is known

as cyberterrorism. Additionally, such computer-contaminating actions have the potential to be fatal or harmful to others. The sentence is life in jail.

Section 67 prohibits the electronic publishing or transmission of pornographic material. This section has expanded and now includes child pornography. According to India's penal law, internet fraud and identity theft are both offences.

In accordance with the IPC, there are sections titled "Making a False Document or False Electronic Record," "Punishment for Forgery," "Forging an Electronic Record to Commit Cheating," "Forging an Electronic Record to Commit Reputation Harm," and "Forging an Electronic Record to Commit Document Forgery." Even electronic documents and recordings are now acknowledged under the Evidence Act. All evidence submitted in court before the enactment of the IT Act was in tangible form.

THE ROLE OF THE JUDICIARY

Due to the rise in cybercrimes, the judiciary, an independent body plays an important to solve conflicts.

Avnish Balaji vs State (N.C.T) of Delhi,[3] 2004.- The Bazee.com case. The CEO of Bazee.com was detained as a result of the website selling a CD with inappropriate content. Additionally, it was offered in Delhi's markets. Mumbai and Delhi police both took action. Despite being accused of breaking sections 292 of the IPC and 67 of the IT Act, the accused was ultimately freed on bail. What sets apart an Internet service provider from a content provider was thus brought up. The burden of evidence lay on the accused since he was the Service Provider and not the Content Provider. It also begs a lot of issues regarding how the police should handle cybercrime cases.

Syed Asifuddin v the State of Andhra Pradesh[4]-Sections 63 of the Copyright Act and Section 65 of the Information Technology Act, which defines a mobile phone as a computer, were allegedly broken by the petitioners. In order to enhance the value of the services provided, each service provider is required to maintain its own System Identification Code and provide a unique number to each device, according to the Andhra Pradesh High Court's interpretation of section 2(1) of the IT Act. Therefore, if the Electronic Serial Number (ESN) is modified, the rules of section 65 of the IT Act are applied.

[3] (2008) 105 DRJ 721: (2008) 150 DLT 769
[4] 2006 (1) ALD Cri 96, 2005 CriLJ 4314

The Bank NSP Case. State By Cyber Crime Police vs. Abubakar Siddique. - In one case, a bank worker who was new to management was getting ready to be married. The newcomer and his fiancée utilised the business' computers. They finally went their own ways. However, the girl set up a phoney email account named "Indian bar associations" on the bank's computer and used it to send emails to the trainee bank's international clients. As a result, the bank suffered significant consumer losses and was later sued in court by those clients. As the source of the emails, it was determined that the bank had committed the crime and oversaw sending the emails to the clients.

My Space Inc. v Super Cassettes Industries Ltd[5]-In this case, the court decided that clause 51(a)(ii) of the Copyrights Act and sections 79 and 81 of the IT Act must be interpreted together harmoniously. It was also determined that Section 81 does not supplant the safe harbour defences offered by Section 79. For intermediaries, specialised knowledge is more important than general comprehension.

State of Tamil Nadu vs. SuhasKutti[6] **-** In one case, the victim was a divorcee who endured annoying phone calls on a regular basis, presuming she would question them about a comment made on a Yahoo message board and followed by forwarded emails. The massage was revolting, distressing, and insulting. Her family's buddy who was drawn to marry her was the suspect. The Additional Chief Metropolitan Magistrate's Honourable Judge has issued the conviction order. The accused was found guilty under Sections 67 of the Information Technology Act of 2000 and Sections 469 and 509 of the Indian Penal Code. After being found guilty, the perpetrator received a two-year term of hard labour. After being found guilty, the perpetrator received a two-year term of hard labour. Cybercrimes have been the subject of several judicial cases all the way up to the Supreme Judicial. As technology develops, criminality also does too, including cybercrime. In addition to trying to eradicate cybercrimes, courts have provided victims with justice.

LACUNA IN THE EXISTING LEGAL FRAMEWORK

- Non-sexual online verbal abuse is not appropriately addressed. General sexist insults are not covered under Sections 499 and 507 of the IPC, which deal with criminal defamation and criminal intimidation for those trolls that are personal. Doxing that does not entail the transmission of graphic content or intimidation is also not included.

[5]Super Cassette Industries Ltd. v. Nirulas Corner House (P) Ltd. (2008) DLT 487
[6]Suhas Kutti v state of Tamil Nadu, C.NO. 4680 of 2004,

Section 66 of the IT Act, which makes hacking illegal, does not directly specify the act of doxing. Online harassment, verbal abuse, and hacking for doxing are all treated as private, isolated offences under Sections 499 and 507 of the IPC and Section 66 of the IT Act. It is important to recognise that this act of violence is being committed against a woman only because she is a woman. As seen in the past, women are mistreated depending on their caste and sexual orientation.

- Section 66E of the IT Act and Sections 354C and 354D of the Criminal Laws Amendment Act of 2013 include an exemption for violence that causes physical injury as opposed to interference with bodily integrity and personal autonomy, as those terms are defined under the other sections of the IT Act and IPC. These parts do not cover "informational privacy"; they solely deal with "physical privacy." Despite being covered by Section 509 of the IPC, "privacy" is only referenced in relation to women's modesty. Most often, sexual violence is viewed to protect women's modesty and promote public morality by lowering obscenity. It can also be revoked at any moment. Gender norms that prioritise protecting women's sexuality over preserving their bodily integrity or personal information are reinforced when sexual abuse and the urge to regulate how sexuality is affirmed and portrayed are coupled. Reading Sections 66-15, 7214, and 43 of the IT Act together results in an economic offence rather than a social or gender infraction.
- Gender-based psychological abuse of women that occurs outside of the home is not recognised by the law. Unrecognised psychological injury is caused when private information is disclosed through a privacy violation that is not sexual.
- In addition, laws like the Protection of Women from Domestic Violence Act of 2005, which deals with instances of psychological abuse in the home and personal relationships, do not cover cybercrime involving women.

CONCLUSION

"The law is not a panacea for all problems." Victims continue to go unjustly without recompense despite a strong legal foundation and their silence. Cybercrime against women is a sharp reminder of what happens in society. The lines separating the offline world from the internet one are blurring. Cybercrime happens because criminals think it is a lot easier approach with fewer consequences. Cybercrime, or criminal activity online, is one of the largest challenges confronting Indian and global law enforcement in the future. As ICT

becomes increasingly popular, elements of electronic crime will surface in all forms of criminal conduct. including those actions presently seen as more conventional violations.

It has already been utilized in various cases of transnational crime, such as drug trafficking, terrorism, human smuggling, and money laundering. As digital evidence is used increasingly frequently, even in classic crimes, we must be prepared to address this new problem. Although the Indian government has made attempts to curtail cybercrime, there is still no sign of an end in sight. The government makes sure the victims get justice or recompense.