(IJDSSH) 2020, Vol. No. 10, Jul-Dec **e-ISSN: 2455-5142; p-ISSN: 2455-7730**

LEVERAGING THE PROVISION IN THE INDIAN CYBER CRIMINAL LAW TO ENHANCE ITS SAFEGUARDS AND PREVENTION APPROACH

Yashika Nagpal

Amity Law School, Delhi (Affiliated to Guru Gobind Singh Indraprastha University)

ABSTRACT

The term "cyber crime" refers to crimes that involve the use of a communication channel or device as a medium, whether it be a laptop, desktop, PDA, mobile phone, watch, or a vehicle, directly or indirectly. Government and corporate leaders should be concerned about cyber-attacks, according to the "Global Risks for 2012" study. The impact of cybercrime on victims can last for years since it is difficult to identify and impossible to stop once it has occurred. This is a word we hear a lot in the media because of the growing popularity of online banking and shopping, both of which need sensitive personal and financial data. Now that we know what this crime is and how it operates against us, we can better defend ourselves. This paper presents a brief overview of all about cyber criminals and crime with its Evolution, Causes, Types, CYBER law, importance of cyber law, cyber law required, components of cyber law, prevent cyber crime, and find conclusion.

KEYWORDS: *cyber law, causes, cyber crime, fraud.*

1. INTRODUCTION

Cybercrime, often known as computer crime, is the use of a computer as a tool for performing unlawful acts, such as fraud, the trafficking of child pornography and intellectual property, identity theft or privacy violations. As computers have become essential to business, entertainment, and government, cybercrime has risen in prominence.

Because computers and the Internet were widely used in the United States at an early stage, most of the first victims and perpetrators of cybercrime were citizens of the country. By the twenty-first century, however, there was not a single village in the globe that had not been affected by some form of cybercrime.

However, new technology also provide new criminal opportunities. Cybercrime differs from traditional criminal behaviour in several ways. One obvious change is the use of digital computers, but this is not enough to make a distinction between different types of criminal behaviour. Fraud, trafficking in child pornography and intellectual property, stealing identities, and invading privacy are all crimes that can be committed without the use of a computer. All of these things were done before the term "cyber" became so widely used. Cybercrime, especially when it involves the Internet, is a new kind of criminal behaviour as well as an extension of previously existing ones.

The vast majority of cybercrime involves an attempt to steal personal, corporate, or government information. A virtual body is a collection of informational properties that defines persons and institutions in cyberspace rather than a real one. This makes it possible for cyberattacks to target virtual bodies, not physical ones. So, in the digital

era, our virtual identities have become indispensable: we are a collection of numbers and identifiers in numerous computer databases held by governments and businesses. Computer crime serves as a stark reminder of how dependent we are on networked computers and how flimsy even seemingly solid concepts like personal identification can be.

Cybercrime's nonlocal nature is one of its most fundamental features; crimes can be committed in countries thousands of miles apart. Because worldwide collaboration is increasingly required to combat transnational crimes, this creates major difficulties for law enforcement. Do people who access child pornographic content on a computer in a country where it is allowed commit a crime in a country where it is prohibited? How and where do criminals do their acts of cybercrime? Cyberspace is nothing more than a more advanced version of the physical area occupied by a telephone call between two individuals. Because it connects every corner of the globe, the Internet provides criminals with a plethora of options for concealing both offline and online. Nevertheless, despite their best attempts to hide their identities and locations, cybercriminals leave evidence about their identities and whereabouts much like people walking on the ground do. However, international cybercrime treaties must be enacted before such evidence may be followed beyond national lines.

A proposed international treaty against computer crime was prepared in 1996 by the Council of Europe and government officials from the United States, Canada, and Japan. International civil libertarian organisations quickly criticised the treaty's clauses mandating Internet service providers (ISPs) to preserve and pass over transaction information on demand, which they said violated their rights. Despite this, work on the treaty continued, and on November 23, 2001, 30 countries signed the Council of Europe Convention on Cybercrime. In 2004, the agreement went into force. There were further standards established in 2002 and implemented in 2006 to deal with terrorist actions as well as racist and xenophobic cybercrimes. Various national legislation, such as the USA PATRIOT Act of 2001, have further increased the authority of law enforcement to monitor and safeguard computer networks.

- **Internet:** Millions of computers are linked together on one worldwide network. Email, browsing the web, chatting, and transferring files are just some of the things you may do with it.
- **Web Browser:** An application for gaining access to a World Wide Web server's information resources. URL, or Uniform Resource Locator, is used to identify an information resource, such as a webpage or an image.
- **ISP:** Users can access the internet through an ISP (Internet Service Provider).
- **IP address:** Devices connected to a computer network are given an IP (Internet Protocol) address, which serves as an identification for that specific system. E.g.,172.17.64.150
- **IP address spoofing:** Also known as IP address forging, it occurs when an attacker gains control of a user's IP address and uses it to carry out their malicious actions. To make the legitimate user appear to be the original source, the hijacker changes packet headers to include the genuine user's IP address in them.
- **Email spoofing;** Email phishing is a common kind of identity theft. Email spoofing occurs when an attacker exploits a user's email address for malicious purposes.
- **Computer virus:** the installation of a malicious computer software in a user's computer that runs against the user's will and has the capacity to corrupt files and spread.
- **Computer worm:** Replicating software is a type of computer programme that spreads to other machines when run. Due to the target computer's security flaws, it typically spreads through network. It's not a virus since it doesn't require an existing software to be attached to it; viruses, on the other hand, can only infect a single machine.
- **Phising:** In other words, it's a heist to get access to confidential information. For example, a user receives an email asking for his bank account information, PAN

number, and 5000INR to process his UK lottery winning claims. He responds by sending the money.

- **Spyware:** A malicious programme is secretly installed on a user's computer in order to collect personal information about that user. Examples of this are Keyloggers2..
- **Computer worm:** Replicating software is a type of computer programme that spreads to other machines when run.

1.1 Cyber Crime in India

Ever since technology's beginning, cybercrime has risen in India at a breakneck pace. Every single day, you'll learn about new online crimes, such as frauds, tricks, and other misdemeanours. The Information Technology Act, 2000 lists several categories of cybercrime in India, indicating a wide range of offences. Many cyber crime cells have been established up in India's main cities as part of the country's compliance with the provisions of the cyber crime act.

Indian cyber crime instances have recently grown as technology has advanced. Kidnapping, fraud, hacking, and data theft are just a few of the crimes done today because to the internet. "Hackers" are criminals who engage in online crimes such as this. A large number of cybercrime cases in India are filed under the Information Technology Act (IT Act).

The pace of digitalization is accelerating, and the Internet has made life simpler for everyone by putting the resources they need at their fingertips. Cyber crimes in India have risen along with other types of criminal activity, including white-collar crime and assaults by terrorist groups. It's made people completely reliant on technology to meet even their most basic needs. Today, anything can be done online, from buying to ordering food to playing games to paying bills.

1.2 Evolution of Cyber Crime

In 1820, a textile maker named "Joseph-Marie Jacquard" created a mechanism called the "Loom" that allowed the reusing of weaving processes, posing a danger to the livelihoods of the employees who were using the equipment. As a result, they carried out a counterattack to demoralise people from using the technology any further than necessary. Traditionally criminal actions like fraud, theft and vandalism are included in cybercrime, as well as web defacement, hacking and web jacking, as well as cyber stalking. "Unlawful activities when the computer is either a tool or a target or both," according to R Nagpal from Asian School of Cyber Law, covers not just desktop computers but also Sophisticated Watches, Mobile Phones, and Personal Digital Assistants. It's impossible to do most modern-day crimes, such as the infamous attack on New York's "World Trade Center," serial bombings, or attacks on India's "The Taj" hotel, without the assistance of computer technology. We can't assess the precise impact of cybercrime on finances and society since it isn't reported in large numbers. Because cyber-attacks have the potential to cause major disruptions to critical infrastructure, such as train and air traffic control systems, stock markets, and financial systems, intelligence agencies are working feverishly to prevent such catastrophes.

1.3 Causes of Cyber Crime in India

When it comes to making large sums of money, cybercriminals usually go for the easier route. It's a crime to hack into a wealthy person's or organization's computer systems and steal critical information, therefore they go after wealthy individuals or institutions like banks, casinos, and financial businesses.

It's tough to apprehend these kinds of offenders. As a result, the number of cybercrimes has increased. The vulnerability of computers necessitates legislation to protect and secure them from cyber thieves. The following are some of the reasons why computers are so weak:

- **Easy to access –** The difficulty with protecting a computer system from illegal access is that the sophisticated nature of the technology makes breaches all but inevitable. It is possible for hackers to acquire information such as access codes, retinal pictures, sophisticated voice recorders, and other biometric data that may deceive security systems and circumvent firewalls.
- **Capacity to store data in comparatively small space –** Because of this, computers

can store enormous amounts of data on a very tiny surface area. As a result, stealing data from any other storage device and reselling it for profit is now much easier.

- **Complex –** Operating systems operate computers, and operating systems are made up of billions of lines of code. Because the human mind is fallible, mistakes can be made at any point in the process. These holes are exploited by cyber thieves.
- **Negligence –** Negligence is a common trait among people. So, it's possible that in our efforts to keep the computer system secure, we've been careless, allowing a cyber-criminal to get access to and control over it.
- **Loss of Evidence –** Data pertaining to the offence is simply disposed of. Since evidence loss is so widespread and evident in cyber-crime investigations, the system is paralysed.

1.4 Types of Cyber Crime in India

When a computer is the target of a cyber attack, cybercrime can be perpetrated against that individual. However, computers can also be used to conduct cybercrime against other people and entities. India's cybercrimes may be divided into four broad categories:

- **Cyber crime against a person:** An electronic domain is used as a means to perpetrate this sort of cybercrime.
- **Cyber stalking:** Stalking refers to a pattern of repeated actions of harassment toward a specific target. Cyber stalking, on the other hand, occurs when a person is harassed online while utilising the internet as a conduit. Rather of actually stalking the target in person, a stalker keeps tabs on that person's internet activity in order to conduct a stalking campaign against them. To harass his victim, a Stalker might use any of the following methods: the internet, e-mail, SMS, webcam, phone call, website, or even video.
- **Hacking:** For the purposes of making illegal gains or misusing one's personal information that is stored on a computer system, hacking means gaining unauthorised access to that person's information without the permission of either the rightful owner of the computer or the person in charge of that particular system. Hacking is any action used to gain access to a computer system or network. Hackers get access to sensitive and personal information about the user. They can also keep tabs on a person's every online move, such as when they log in, when credentials are added, and when they do financial transactions, for example.
- **Cracking:** Crack is a term used to describe the process of cracking software. To crack anything, you must remove the Copyright protection code from a piece of software digitally. This stops pirated or duplicated software from running on computers without permission from the software seller or owner. A cracker is someone who engages in such behaviour, as opposed to a hacker. In order to get around the legislation, Cracker tampers with the computer.
- **Defamation:** Defaming someone's reputation in society through the use of a computer or the internet is known as online or cyber defamation. This is accomplished through the use of defamatory statements on social media, obscene images and videos, and disparaging e-mails sent to the victim's contacts, among other methods.
- **Online Fraud:** One of the most frequent kinds of cybercrime is online fraud. phishing sites are used to collect sensitive information like a person's bank account details and then take funds from the victim's bank account. Scams involving online lotteries are all the rage these days, with Nigerian lottery scams being one such example.

(IJDSSH) 2020, Vol. No. 10, Jul-Dec **e-ISSN: 2455-5142; p-ISSN: 2455-7730**

- **Dissemination of Obscene Material:** The dissemination of pornographic or obscene items via social media is included in this definition. It involves hosting websites with sexual content, which tends to deprave or corrupt people's brains.

- **Child pornography:** It is also a cyber crime to distribute anything that might deprave the minds of minors. Electronic devices are being used to generate, distribute and/or access pornographic content, which has the potential to degrade the brains of children.

- **Spoofing:** Spoofing is the process of making false claims about the source of data. An email or SMS sent from one source appears to have come from another, even if it was sent from the first. This method is used by cyber thieves to steal personal information such as bank account numbers and other financial information from its victims.

- **Phishing:** It entails sending unsolicited emails to the user under the guise of an established company in order to collect sensitive personal data.

- **Cyber Crime against property:** A computer or other electronic equipment is used as a means to commit property crime known as cybercrime. Rather than only physical property, the term "property" refers to moveable and intangible assets like computers and other forms of Intellectual Property.

2. CYBER LAW

Cyber law, also known as information technology law, is also referred to as Internet law. Cyber law, according to the definition, is a legal system created to address concerns relating to the Internet, computing, and cyberspace. A good place to start learning about Cyber Law is: In a 'paperless world,' there are 'paper laws.'

There are many different elements of cyber law. These include: intellectual property rights; contracts; jurisdiction; data protection regulations; privacy; and free speech. Digital circulation of software and information, as well as the security of online transactions, are all controlled by it. E-documents have legal validity thanks to Cyber Law. E-commerce transactions and electronic filing are made possible by this framework. The Cyber law is therefore a legal framework for combating cybercrimes, which may be seen as a whole. Due to a rise in the use of E-commerce, it is critical that adequate regulatory standards are put in place to guarantee that there are no malpractices.

Country and jurisdiction-specific cybersecurity legislation is vastly different. Depending on the crime committed, penalties range from a fine to incarceration for the same offence. It's critical that individuals understand their country's cyber laws so they're up to date on all they need to know about cybersecurity. The Computer Fraud and Abuse Act of 1986 was the first cyber legislation to be passed, and it made it unlawful to gain unauthorised access to computers or use digital information without permission.

2.1. The importance of Cyber Law

In the same way that all laws have regulations dictating how people and organisations should utilise computers and the internet, cyber law does as well. Other regulations, on the other hand, help individuals avoid becoming victims of cybercrime perpetrated by nefarious actors. Laws put in place across the world help, even if they can't stop all cybercrime completely. How important is Cyber law now and how did it get that way? The following points help illustrate the significance of cyber law:

- It dictates all actions and reactions in Cyberspace.
- All online transactions are ensured to be safe and protected
- All online activities are under watch by the Cyber law officials.
- Data and property protection for individuals, businesses, and the government
- Helps curb illegal cyber activities with due diligence
- Every activity and reply in cyberspace has some sort of legal ramifications.
- Keeps track of all electronic records
- Helps to establish electronic governance

2.2 Cyber Law Required

Over 4.66 billion individuals will be connected to the internet by the beginning of 2021. This figure is rising at a 7% yearly rate. This also implies that about 8,75,000 new users join the system every day. Because of the rapid growth in the use of Cyberspace, enforcing strong cyber regulations is essential for keeping users safe and secure. The Internet is the only thing that can keep up with our fast-paced world. Despite its origins as an informational tool, the internet now aids in communication and business as well. Because cyberspace is very complex and evolving on a daily basis, it has been widely used, and as a result, the number of cybercrimes is bound to rise. with the task of keeping things organised when doing things online. It is up to the victim/firm to take action if someone is proven to be violating rules or Cyber laws.

2.3 Components of Cyber Law

Data and privacy must be protected on both a personal and professional level. Cybercriminals are constantly interested in personal and financial information. Any unauthorised use of this data is against the law, which is why there are regulations in place. To protect your data and privacy, follow these simple actions.

- The use of two-factor authentication on financial platforms and in any other forum where it is available.
- Initiate Virus protection software.
- Use only verified payment methods on reputed websites.
- Avoid giving out personal information

Cybercrimes- Any criminal activity carried out through the use of a networked technical equipment falls under this category. These crimes include hacking, extortion, harassment, and money laundering over the internet and in networks, to name just a few.

Intellectual property- Anything intangible and typically patented or copyrighted that belongs to an individual or group is considered intellectual property. Cyber theft, on the other hand, refers to the theft or unauthorised use of the same intangible assets through the internet.

Electronic and digital signatures- Electronic signatures are now used by the majority of people and businesses to validate electronic records. This has established itself as a dependable and recurring service. The unauthorised use of this signature by a third party is a kind of cybercrime.

3. PREVENT CYBER CRIME

To effectively combat cybercrime, law enforcement authorities, the information technology sector, information security groups, internet service providers, and financial institutions must create multi-dimensional public-private cooperation.

Cyber criminals, in contrast to their counterparts in the physical world, are not engaged in a power struggle. As a substitute, they collaborate to enhance their abilities and even assist each other land new jobs. As a result, traditional law enforcement tactics cannot be employed to combat cyber crimes in India.

- **Use Strong Passwords:** Avoid writing down your passwords and usernames since they should be unique for each account.
- **Keep Your social media accounts private:** Don't forget to keep your social media accounts secret (such as those on Facebook, Twitter, and YouTube). Verify the security settings on your computer. Take caution with the information you provide on the internet. Whatever you post on the Internet will remain there in perpetuity.
- **Secure your Mobile Devices:** Many individuals aren't aware that harmful software, like computer viruses and hackers, may also infect their mobile devices. Be cautious while downloading apps, and only do it from reputable websites. Additionally, make sure that your operating system is up-to-date at all times. Consider using a secure lock screen in conjunction with anti-virus software. Otherwise, if you lose your phone or leave it on the table for a few minutes, anybody may see anything you've stored on it. Even if malicious software isn't installed, it's possible that someone will use your GPS to follow your every step.

- **Protect your data:** Encrypt your most critical files, such as bank documents and tax returns, to keep your information safe.

- **Protect your identity online:** Being overly careful when it comes to preserving your online identity is preferable than being underly cautious. Giving up personal information such your name, address, phone number, and/or financial information via the internet should be done with extreme caution. When making purchases or other types of transactions online, ensure certain the websites you are using are safe. Using/accessing social networking sites also entails turning on your privacy settings.

- **Keep your computer current with the latest patches and updates:** Applying patches and other software fixes as soon as they become available is one of the greatest methods to keep hackers away from your computer. By upgrading your computer on a regular basis, you keep hackers from exploiting security weaknesses (vulnerabilities) to get access to your system.

- **Protect your computer with security software:** A variety of security tools are required for even minimal internet safety. Firing up a firewall and installing an antivirus application are both critical security software components. The first line of defence for your computer is generally a firewall. Your computer's network access is restricted by this programme. A firewall acts as a type of "policeman" for your computer, keeping an eye on all Internet traffic and only permitting communications that it deems safe while preventing "bad" traffic like assaults.

4. CONCLUSION

Case examples have been used to support our descriptions of various elements of cybercrime in this study. Conclusion: Cybercrime is far more terrible and destructive than traditional crime. In today's computer-dependent world, every nation and citizen must be knowledgeable about cybercrime, criminal psychology, and the regulations that go along with it. "The best defence against a hacker is a good offence against oneself." The violation of IPC 501 under the IT Act absolves the intermediary (ISP) of responsibility. The use of anti-virus software and the installation of firewalls protects us from such criminal activity. Installing software that isn't absolutely necessary is a bad idea. It's a good idea to keep backups and security settings current on a frequent basis. Internet privacy is ensured by not disclosing personal information such as one's complete name, address, or email address to an unknown party.

(IJDSSH) 2020, Vol. No. 10, Jul-Dec **e-ISSN: 2455-5142; p-ISSN: 2455-7730**

REFERENCES

1. Authored by Laxmi Narayan Opposite NKT college, Ganpat JairamKharkar Marg, Shivanjali CHS,Kharkar Alley,Thane, Maharashtra.
2. Authored by Dr. Mrs. Pratibha Cyber laws and Information Technology Dr. Mrs.
3. Cyber Crimes And The Cyber Laws in India.Cyber Stalking & the Impact of its
4. An overview of cyber laws Vs cybercrimes: in Indian.
5. cyber law and cyber security in developing and emerging economies Zeninab karake- Shalhoub, Lubna Al Qasimi.
6. March 2012K. Elissa, “Title of paper if known,” unpublished.
7. Birk, D.; Gajek, S.; Grobert, F.; Sadeghi, A.-R.; , "Phishing Phishers - Observing and Tracing Organized Cybercrime," Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on , vol., no., pp.3, 1-5 July 2007
8. McCombie, S.; Pieprzyk, J., "Winning the Phishing War: A Strategy for Australia," Cybercrime and Trustworthy Computing Workshop (CTC), 2010 Second , vol., no., pp.79,86, 19-20 July 2010.
9. Neufeld, D.J.; , "Understanding Cybercrime," System Sciences (HICSS), 2010 43rd Hawaii International Conference on , vol., no., pp.1-10, 5-8 Jan.2010
10. Mesko, G.; Bernik, I.; , "Cybercrime: Awareness and Fear: Slovenian Perspectives," Intelligence and Security Informatics Conference (EISIC), 2011 European , vol., no., pp.28-33, 12-14 Sept. 2011
11. Cybercrime at a glance," Spectrum, IEEE , vol.43, no.4, pp.17,, April 2006
12. Yasinsac, A.; Erbacher, R.F.; Marks, D.G.; Pollitt, M.M.; Sommer, P.M., "Computer forensics education," Security & Privacy, IEEE , vol.1, no.4, pp.15,23, July-Aug. 2003 doi: 10.1109/MSECP.2003.1219052
13. S.C Bhatt, D. Pant, "Cyber Crime in India," IJARCS, vol. 2 No.5 pp. 153-156, Sept-Oct 2011.
14. M. Sharma, Pragati. G, “Challenges and Countermeasures for Web Applications” , IJARCS, vol. 2 No.3 pp. 381-384, May-June 2011.