INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 4

2021

Critical Analysis of Cyber Crime with reference to Lack of Awareness in the Society

MR. JYOTIRMOY BANERJEE[1] AND MS. POOJA BANERJEE[2]

ABSTRACT

The use of the mobile phones, internet and social media has become a part of everyday life for most of the people in carrying out daily transactions. Internet users are growing enormously, as is cybercrime. Cybercrime is a crime committed with the help of computers and networks. The threat of cybercrime is a reality that always exists and develops both in the personal and professional spheres. With the advent of internet, old evils have been given a new face. The aim of this study is to raise awareness of cybercrime in today's world and to raise awareness of increased cyber security. This paper tries to analyze cybercrime awareness among the Internet users of several of various ages and educational backgrounds. It is presumed by the author that there exists a relationship between the age group of the respondents and the level of education. Therefore, it is the duty of all the internet users to be aware of cybercrime, be secure from any such crime and also help others by creating awareness among people.

Keywords: *Cybercrime, Cyber security, Information Technology Act, Awareness, etc.*

I. OVERVIEW

In India, the internet users are rapidly growing rapidly which created new opportunities in entertainment, business, sports, education and more. Due to the increase in internet use, companies are breaking down barriers in local markets and reaching customers the entire world. Computers are used in companies not only as a tool to process information, but also to achieve strategic and competitive advantages. It can be used for both constructive and destructive reasons. Misuse of the internet has led to a new era of crime that is addressed by the Information Technology Act, 2000. As information becomes more accessible around the world, it also becomes more vulnerable to get misused by the people who misuse the information and cause harm or loss to people. India is on the radar of cybercriminals with increasing cyber-attacks against Indian companies. India ranks third as a source of malicious activity on the Internet after the United States and China. It ranks 2nd as a source of malicious

[1] Author is an Advocate at Lucknow High Court, U.P., India.
[2] Author is an IT Faculty at Billabong High International School Malad, Mumbai, India.

 [ISSN 2581-5369]

code, and 4th and 8th as a source or source of web and network attacks. As per CERT- In[3], 27, 482 cybercrime cases, such as phishing, malicious code, ransom-ware, etc. were reported during the initial seven months of 2017.

The increasing frequency of internet usage has created problems for people who spend hours surfing the internet. It has also opened the door to a wave of cybercrime. When people are not cautious about the problem, then it causes financial, emotional, moral or ethical harms to them. Apart from fighting cybercrime, another issue that needs to be focused on is making Internet users aware of "*cybercrime and security*". Therefore, it is important to know: "W*hether people really understand that they are vulnerable to various kinds of cybercrimes? And if they understand their vulnerability then, to what extent they? And what steps they can take to secure themselves and others from such crimes?"*

II. KNOW ABOUT CYBERCRIME

Cybercrime is a term that is used to refer an unlawful or criminal act that is committed through electronic communications media, where a computer or network is used as a tool or target or both. The term "Cyber Crime" is not defined under IT Act, 2000 or IPC, 1806 but it deals with offences that are related to cybercrimes. It is due to the reason that the types of cybercrimes are so widespread that it is almost impossible to limit the definition. Some of the common cybercrimes nowadays that are plaguing the society are pornography, bank frauds, counterfeit, etc. Cases against cybercrimes can be registered under:

- IT Act, 2000.[4]
- IPC, 1860.[5]
- Other State Level Legislations (SLL).

Cyber cells have been established to work on the cybercrime cases.

Categories of Cybercrimes

On a roughly basis, there can be 4 main categories as per their purpose and impact:

- ***Crimes against individuals***

Crimes that are committed to harm a particular individual comes under this category that includes hacking, cracking, harassment through mails, online stalking, bullying, defamation,

[3] Indian Computer Emergency Response Team.
[4] Information Technology Act, 2000.
[5] Indian Penal Code, 1860

 [ISSN 2581-5369]

spreading obscene material, spoofing, frauds, cheatings, pornography, etc.

- ***Crimes against property***

Crimes that are committed to harm or destroy someone's property, falls under this category. The crimes under this category includes crimes relating to intellectual property, computer forgery, vandalism, sending virus or malicious content, etc in order to destroy the victim's property.

- ***Crimes against government, firm, company or group of peopl***

Crimes such as cyber terrorism, dissemination of pirated software, web jacking, logic bombs etc, are some of the ways that can cause injury to government, firm, company of group of people. The motive behind such crimes is to spread terror among the people.

- ***Crimes against society***

Any crime that impacts the individuals has a direct or indirect impact on the society therefore any above mentioned crimes will be included under this category.

III. OVERVIEW OF CYBER LAWS IN INDIA

Since cybercrimes are often committed against entities defined and addressed in the Information Technology Act, it also provides for the punishment of such crimes. IPC is the central law dealing with conventional crimes in India. As the scope of this crime continues to expand in the face of the technological revolution, any of these forms of crime can easily be classified as cybercrimes. Therefore, cybercrimes in India are treated according to the following two laws:

1. IT Act, 2000

Information technology was identified as a key factor in the search for economic excellence and growth in the early 2000s. Central and state governments stimulated the growth of IT training centers. Basic computer skills were required in centralized schools, and soon the entire population was provided with basic computer skills. Investments in the development of the IT sector have paid off quite quickly and the IT industry is growing rapidly in the country. The IT industry is tertiary and supports the functioning of the primary and secondary sectors of the economy, while some professionals set up companies and have independent activities in the form of software giants and consulting services, a large part of the transition industry population is IT literate to meet the IT requirements of these organizations. However, a small percentage of the population uses IT experience for certain ulterior motives. IT Act, 2000 was enacted to meet the needs of the country's growing IT community and to undergo investigation

 [ISSN 2581-5369]

and to provide punishment to the last element that succumbs to misuse of information technology.

Chapter 11 of the Information Technology Act[6] describes and discusses various cyber crimes in detail and regulates their penalties. Here are some of the common crimes punishable under IT law:

- ***Tampering computer source documents[7]***

Section 65 of the Act provides punishment or penalties for hiding, destroying, and altering data, the maintenance and storage of which is not required by law, any person committing such crime can be punished with an imprisonment that may extend up to 3 years or with fine that can be extended to 3 lakh rupees or both.

Eg.- If any data that is required as an evidence to be brought to court, alteration of content or production of counterfeit copies may result in up to 3 years in prison and a fine.

- ***Identity theft and cheating by Personation[8]***

Using electronic signatures or passwords illegally of any individual can be termed as "identity theft" which can be punished with an imprisonment that can extend up to 3 years and fine that may extend to 10,000. Cheating by personation can also be punished with imprisonment extendable up to 3 years and fine.

- ***Privacy Violation***

Right to privacy is a fundamental right under Article 21[9] of the Indian Constitution as per the Supreme Court's decision. Therefore, if any act that infringes privacy of a person, is violation of the fundamental right of that person. IT Act punishes the violator with 3 year imprisonment and fine.[10]

- ***Cyber Terrorism***

Threats to the sovereignty of a nation through the use of computer resources are known as cyber terrorism. Often the use of computer programs such as viruses and others that supports cyber-terrorist actions, these actions tend to harm people's lives and can even result in death. IT Act provides punishment of cyber terrorism with life imprisonment.[11]

[6] Sec 65- Sec 78, Information Technology Act, 2000.
[7] Sec 65, IT Act, 2000.
[8] Sec 66C, IT Act, 2000
[9] INDIAN CONSTITUTION, Art. 21.
[10] Sec 66E, IT Act, 2000.
[11] Sec 66F, IT Act, 2000.

 [ISSN 2581-5369]

- ***Spreading Pornography***

The legal transmission of pornographic content is very strict because the consequences of transmitting pornographic content have been assessed by lawmakers, as the transmission will have a lasting and severe impact on the lives of the victims. IT Act punishes any person who has done the crime for the first time with the imprisonment of 3 years along with 5 lakh rupees fine and the person who has committed the same crime for the second time with imprisonment of 5 years and 10 lakh rupees fine.[12]

- ***Child Pornography***

The victims of these crimes are children less than the age of 18 years. For the first time convict, the Act prescribe punishment of 5 years and 10 lakh rupees and for the second time convict, the punishment is for 7 years and extra 10 lakh rupees.[13]

- ***Compensation for a corporate who fails to protect data***

When a company who is holding sensitive personal data fails to protect the same then it is liable to pay compensation.[14] A company that is given the hold of personal data of people should apply reasonable security measures so that the loss of data can be prevented and if they do not do so and the data gets lost then they will have to pay the compensation for the same.

The Central government should issue certain guidelines to provide certain rules and to recommend security strategies and practices to guarantee that the contradiction of the different orders of the resolution doesn't occur. The Act additionally empower the legislature to make such rules that provide better execution or implementation of the Act.

2. Indian Penal Code, 1860

The amendment in IPC in light of the Information Technology Act, 2000 was made to include e-record and e-documents within the definition of records and documents so that if there is any falsification in e-records or e-documents, then it will be considered as an offence.[15]

IV. IMPACT OF CYBERCRIMES

1. Impact on society

Increasing cybercrimes are a sign of caution for the society. It is important to note that when a cybercrime occurs in a society then it not only impacts that particular person or his family but

[12] Sec 67, IT Act, 2000.
[13] Sec 67-B, IT Act, 2000.
[14] Sec 43-A, IT Act, 2000.
[15] Sec 192, 204, 463, 464, 468-470, 471, 474, and 476, etc were added after the amendment.

 [ISSN 2581-5369]

also to the society as whole. We all rely upon the internet and stay for longer times and therefore it is very easy for anyone who wants to commit any crime against any person online. Committing a cybercrime is very easy nowadays and the online users are vulnerable to get victimized to any kind of cybercrime. If even a single individual gets victimized to cybercrime, it has an overall impact on society. Cybercrimes can cause potential disturbance to the society and it can cause lose of any valuable such as money, peace, property, etc.

2. Impact on socio-eco and political riders

Crime is an offence that not only impacts the victim or its family but also to the entire society. It impact the social, economic and political conditions of the country. Everything is interconnected, therefore if due to any reason any disturbance is caused, then it impacts the social, economic and political conditions of the society or country.

3. Impact over teenagers

Teenagers who are users of internet have a fear of cyber-bullying as they are most vulnerable to cyber-bullying. Cyber-bullying is a term referred to acts of sending threatening or negative messages, comments or pictures that causes tension, problem or disturbs the peace of the victim. Mostly the female teenagers are the ones who face cyber-bullying. Cyber-bullying can be done through sending messages online via Facebook, Instagram, Orkut, and other social media apps.

4. Impact over private industry

Cybercrimes are used to wrongfully get hold or acquire the property, money or important data of any private company. Hackers can hack, or get access of the computer resource of the industry and get hold of the information that can help the hacker to blackmail the private company and ruin its reputation, damage property or anything that is of important value to the company.

5. Impact over youth

Youth nowadays spend time over internet on social media to interact and get connected with other people. Youth use social media apps to get connected with people of outside world. They connect to people become friends with them, cheat, have conversation with them and get attached with them. They get connected emotionally with each other but sometimes a person misuses the emotion of others and uses it to cyber-bully the person or does anything to cause depression, mental torture or any kind of mental or monetary damage to the victim.

Excessive use of social media for interaction can lead to change in the style of writing or using

words. On social media, formal writing is not used for interaction and therefore through excess use of informal language, it is quite possible that a person gradually loses its catch upon the formal writing.

Another consequence of social media is cyber-bullying. Youths who interact with any anonymous person and share with them their personal information, can anytime misuse any information to blackmail or bully them. They can harass people online especially female and cause them mental depression that to such an extent that they can cause self-harm.

Youths are also vulnerable to sexual solicitation as they engage in sexual chats, rooms or sexual relationships online with people that may misuse the photos, videos or take recordings and use them as a weapon against the person.

V. CRITICAL ANALYSIS TOWARDS CYBER ATTACKS

Crime, its level, ways of committing crimes, weapons for committing crimes and motive keep changing. Crime and society are co-related to each other, i.e., they both are dynamic. With significant educational growth and exponential increase in society's cumulative technology, offenders have also got themselves upgraded and they use such new technologies to commit any offence. New crimes are being committed that affect many people and conventional offences are committed nowadays with great precision and with available modern technologies. Cybercrimes are nowadays committed even more than the conventional crimes and that is why it has become a hot legal topic today. Cybercrime laws tries to eliminate injustices committed against the community through the instruments of legislation and their implementation.

The ways to commit cybercrime also keeps evolving therefore in order to cater the problem of new crimes, it is very important that the laws relating to cybercrimes keeps getting amended and including punishments for all the new types of cybercrimes. Eg. - Section 66C and Section 66E.

The Information Technology Rules (Adequate Security Practices and Procedures and Sensitive Personal Data or Information) of 2011 complement the present procedure or laws that deal with protecting data in India.

Rule 8(1) speaks of the need for good security mechanism.

Following the debate over the violation of Aadhar's privacy rights, the 2017 Data Protection Act was revised by The Ministry of Information Technology, where the Government of India published "*Guidelines for Securing Identity Information and Sensitive Personal Data or Information in accordance with the AADHAR Act, 2012 and the Information Technology Act,*

2000."

Cybercrimes are such kind of crimes that a person can commit to anyone residing at any place in the world. It is very important that people be aware of all kind of crimes that can occur online and they secure themselves from such crimes. Lack of awareness is a powerful weapon that the offenders use and cause harm to people. Many teenagers, youths and even grown ones have encountered such experience of cyber bullying, hacking, or any other kind of cybercrime. Instead of hiding such circumstances, people should be vocal about such instances and create awareness in the society so that no other person has to face or undergo same trauma as they did. People become victim to cybercrimes even after being educated so it is very obvious to understand that those who are not well-educated and use social media for entertainment purpose, they are more vulnerable to such crimes. Therefore, it is very important that people who are in rural areas and are not properly well-educated but using internet for any purpose, they should be aware of the types of online frauds, scams and crimes that can be committed and how to be safe against them.

How to spread awareness?

1. Be as much cautious as you can.
2. Never share your personal information that is to be confidential with anyone online.
3. Never get intimidated by any person who blackmails or odes anything to get possession of any valuable thing.
4. Be vocal about any such incidence that has happened with you so that other becomes aware and be safe from any such act.
5. Call or inform police regarding any kind of cyber-crime.

VI. Conclusion

The future of the internet is still caught between criminals and ordinary users. Fear of cyberspace the apocalypse still abounds while the potential amount of damage that a large-scale fraud can cause is almost unlimited. These concerns should be appropriately mitigated by the knowledge that:

Problem solved, although maybe not fast enough. The benefits of the internet are there it has been proven in countless and countless ways which we hope is enough to make sure that doesn't happen a desert of criminal activity and a stronghold for the evil one. Government is still important role, but most of the prevention should be done by the software vendor and those who have the ability to stop fraud. Reliance on consumer education programs only affects a

Percentage of possible victims.

The rest should be automatically protected by actions that do not emphasize emphasis and require significant participation. Security should be simple and effective, if any I am working. Is cybercrime still a topical issue after ten years? It makes sense, but if the internet continues to grow, it must be addressed so that the reality of cybercrime is addressed proportionate, if not better, to the actual crime.

*****

 [ISSN 2581-5369]