Page 1737 - 1744 DOI: https://doij.org/10.10000/IJLMH.113008

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 2

2022

The Rise in Cybercrimes: A Major Threat to Human Race

MEDHANSH MISHRA[1] AND RANEETA PAL[2]

ABSTRACT

The man deserves all the credit for receiving god's gift, with both his hands, which endows human beings with the capability of using the brain efficiently. By this only advent of technology was possible with making communications faster underlying purpose behind it. But this purpose appears to have been overshadowed by the negative aspect of technology i.e. cybercrimes as per the recent trends which show an upsurge in the commission of crime rate over cyberspace. In stark contrast to the times when there were very few Cybercrimes committed we are witnessing a situation wherein every year cybercrimes are crossing their previous tally. With almost no fear in the mind of getting caught criminals are carrying out these activities backed by their ill intentions. The world of the internet facilitates cyber crimes in two ways firstly its being borderless makes people of several countries prone to cyber-attack and secondly when it provides the offender with the luxury of committing a crime just by sitting in his room which makes it difficult on part of authorities to get hold of the culprit. This horrendous increase in cybercrimes poses a threat to the entire human race and immediately calls for change in the manner we use our gadgets. This write-up describes the ground reality of cybercrimes in India. Certain precautionary measures have been entailed in this write-up which every individual should take on his part to save the human race from the detrimental effect of cybercrimes.

I. INTRODUCTION

“Change is only constant" this quote is of great relevance as far as the evolution of human beings is concerned. In ancient times when basic amenities were scarce such as food, clothes, shelter etc. and where the major question was survival man entered into the era of a virtual world with Technology being the driving force behind it. Man being in an advantageous position as compared to other creatures by his being able to use his mind in a rational manner has left no stone unturned to use it to its fullest potential. Advancement in technology which has been made in recent times is one appropriate example of this. With technology coming in we witnessed the advent of cyberspace which then was introduced just with the idea of using

[1] Author is a student at Manipal University Jaipur, India.

[2] Author is an Assistant Professor of Law at Manipal University Jaipur, India.

it as an alternative to certain tasks which used to take long hours to get done in the physical world. Email is one such example of this which came as a substitute for handwritten letters to make communication faster. But with time passing by cyberspace seems to have taken an edge over the physical world.

In present times, cyberspace has become one such platform that has become a whole new world in itself and the internet is the most common one (cyberspace), which renders it impossible for one to imagine the smooth functioning of his life's normal daily activities, instances are many to support this online payment transactions, purchasing goods through e-commerce websites, business meetings done through video conferencing apps are to name a few. These are examples which are of utmost necessity if we take into consideration other aspects in which internet is being used then not even a single domain of life is left out which does not require internet to be used. It can be said that human life has become internet-centric in recent times. There is not even any problem with cyberspace taking centre stage till the time it is for benefit of people but the problem comes in when the negative aspect of this technology-driven world comes to the forth i.e. cybercrimes.

Cybercrime can be defined as a crime that takes place over cyberspace called the internet. In other words, we can describe it as crimes when are done through the mode of technology[3]. As per the recent report by National Record Crime Bureau 'Crime in India 2020', there has been a rise of 11.8% in cybercrimes over the previous year[4]. And there is a likelihood of a rise in cybercrimes in near future, keeping the increase in technology-based crimes in mind, there is a need that people to use their technology devices with a bit of care. Viz. (people should not be using their gadgets without any antivirus installed.) Awareness among people regarding safety measures while using their gadgets seems to be of utmost importance. In this write-up, the author has mentioned what safety measures can be taken on part of individuals to keep themselves protected from cyber threats.

II. Evolution of cybercrime

(A) Cyberspace

Cyberspace refers to a virtual world of computers and a mode in an electronic form through which communications around the globe are facilitated. Cyberspace consists of a large computer network that is made up of multi-computer sub-networks that apply computer

[3] Animesh Sarmah, A Brief Study on Cyber Crime and Cyber Laws of India, 04, IRJET,1633, 1633, (2017).

[4] How Covid affected the crime graph in 2020, TOI, Sept. 15, 2021.

protocol to carry out data transmission and communication activities[5].

The above referred definition makes one understand the technical aspect of the term "Cyberspace". If it has to be put in a lucid manner then it can be said that cyberspace is a platform within which all sorts of works in which the use of the internet is required are performed.

(B) Emergence of cybercrime

The late '80s was that era when there was for the first time seen a rise in the number of cybercrimes which was done through the proliferation of email which as a consequence made it easier to send a number of viruses to other's inboxes.[6]

The advent of web browsers' in the '90s witnessed a huge surge in the rate of cybercrime. In this era, the method which was in vogue was that of distributing viruses through the medium of internet connections.

In the 2000s with the coming of social media into a common man's life cybercrime flourished. Offenders in this era have indulged themselves in committing ID fraud. What offenders do in this is that they try to steal personal information of people such as bank account essentials and steal their hard-earned money thereon.[7]

(C) Nature and manner of cybercrime

Cybercrime falls into the category of a criminal offence. These crimes are committed usually through computers with the help of the internet. Intentioned acts through malware are being carried out. Stalking through online mode and committing ID fraud with people and thereon making them suffer huge losses by debiting money out of their account in an illegal manner are a few examples showing the adverse impact of cybercrimes.[8]

Contrary to the mode of commission of crimes that was there in the past times cybercriminals perform illegal activities through online mode. In earlier times in order to scam people help of letters, telegrams, etc. was taken. Now contrary to that crimes are being committed through the computer by sitting in a room and at the same time affecting a large number of people as compared to the former time.[9]

[5] What does cyberspace mean, Techopedia, Sept. 30, 2020, https://www.techopedia.com/definition/2493/cyberspace.

[6] SauvikAcharjee, The Evolution of cybercrime: An easy guide, jigsaw academy, Feb. 13, 2021, https://www.jigsawacademy.com/blogs/cyber-security/evolution-of-cybercrime/.

[7] *Id.*

[8] Cyber management, The nature of cybercrime and scams, NST cyber, https://netsentries.com/the-nature-of-cybercrime-and-scams/.

[9] *Id.*

The perspective with which cybercriminals indulge in criminal activities is that they consider it as an act that will provide the maximum benefit with a minimum amount of risk involved. Now a question might arise why has this been considered by the offenders as having a low-risk factor, the reason lies in the fact that, unlike conventional crimes, the person who is committing cybercrime need not be present in person at the time of the commission of the crime so there is no chance of his being caught red-handed. Moreover, as the internet is not confined within any borders so the likelihood of a person sitting in America and being indulged in cybercrime activities being executed in India can never be denied. And in the case when such is the scenario it becomes almost impossible to find the real culprit.[10]

(D) The magnitude of cybercrime

A few years back, when technological devices were not so commonly found in hands of an ordinary man there were hardly any cases of cybercrime to be seen. But as technological devices become more accessible and people started to understand the mechanism on which they work we have witnessed a lot of activities being carried out through the mode of technology be it negatively or positively. This friendliness with technology tools has two aspects attached to it. One aspect reflects the group of people who used technology as a tool for the betterment of their lives and then there is another group of people, which are covered under the second aspect, who have used it as a tool for fulfilment of their ill intentions.

In the initial days, the people who used technology for good were quite high in number as compared to the ones who use it in order to commit crimes. But there has been a change in this count in the past few years. We have witnessed the magnitude of cybercrimes rising day by day and affecting a lot of people in recent times. Above mentioned statements are supported by data in the following lines.

National Crime Records Bureau has stated in-home panel report that there has been an increase in cybercrime of 11% in the year 2020 as compared to the past year i.e. 2019. According to the report, the total number of cases of cybercrime which were registered in 2020 was fifty thousand and thirty-five (50,035) while this number in the year 2019 stood at forty-four thousand seven hundred and thirty-five (44,735).[11]

If divided category wise then 60.2% of the total cases of cybercrime were of fraud i.e. thirty thousand one hundred and forty-two out of total. While cases of sexual harassment stood at

[10] *Id.*

[11] 11% jump in cybercrime in 2020, B. S. feb.11, 2022.

6% cases of extortion were reported at a rate of 4.9%.[12]

Let us have a look at, through data uploaded by the National Records Crime Bureau, the increasing rate of cybercrimes over the past few years. According to the report, in the year 2014 total number of cyber crimes registered in India stood at nine thousand six hundred and sixty-two (9622)[13]in the year 2015, this number increased to eleven thousand five hundred and ninety-two (11592)[14] in the year 2016, it was marked at twelve thousand three hundred and seventeen (12317)[15] while it saw a sharp rise in the year 2017 when the number of cybercrimes registered went up to twenty-one thousand seven hundred and ninety-six (21796)[16].with the addition of five thousand five hundred and fifty-two (5452) more cases, the total number of cases in the year 2018 remained at twenty-seven thousand two hundred and forty-eight (27248).[17]

By looking at this data it is pretty much evident that cybercrimes are rising at a rapid pace.

III. CYBERCRIMES UNDER INFORMATION TECHNOLOGY ACT 2000

Section 65, whoever knowingly causes himself or causes by another concealment, alteration or destruction of computer source code when the law requires it to be maintained shall be punished[18].

Section 66, offences related to the computer, if by any person ay act is done referred to in section 43 with the dishonest or fraudulent intention he shall be punished.[19]

SECTION 66B, Anyone who with dishonest intention receive or retain any computer resource which is stolen shall be punished.[20]

SECTION 66C, When with fraudulent or dishonest intention use is made by one person of another’s password or identification details he shall be punished.[21]

SECTION 66D, Person who cheats by personating using a computer resource shall be punished.

[12] *Id.*
[13] Crime in India statistics, National Crime Record Bureau, Oct. 30, 2017, https://ncrb.gov.in/sites/default/files/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf.
[14] *Id.*
[15] *Id.*
[16] Crime in India statistics, National Crime Records Bureau, Dec. 26, 2019, https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%201.pdf.
[17] *Id.*
[18] The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009.
[19] *Id.*
[20] *Id.*
[21] *Id.*

SECTION 66E, Anyone who with having an intention or with knowledge captures personal or private images of a person or transmits or gets them published and does not take consent of the person for this shall be liable for punishment.[22]

SECTION 66F, Anyone who indulges in the commission of cyber terrorism shall be punished.[23]

SECTION 67, Anyone who publishes or transmits material that is obscene in electronic form shall be punished.[24]

SECTION 67A, Transmission or publication if done by a person of material which contains any act which is sexually explicit then such person shall be liable to receive punishment.[25]

SECTION 67C, whoever indulges in publication or transmission of any material which depicts children in an act that is sexually explicit in electronic form shall be punished.[26]

IV. Precautionary measures

If the question is can an individual prevent cybercrime then the straightforward answer is NO. However, some precautionary measures are there that an individual should take while using the internet in order to protect himself from cyber attacks.

1. Software update

This is quintessential for one to keep his system's software updated. What often has been seen is that any sort of defect or flaw in software is what makes cybercriminals gain access to the system. Updating software at regular intervals will nullify the possibility of the system getting exposed to cyber-attacks.[27]

2. Reveal less

Personal information should remain behind the curtains. For one might be absolutely clueless while mentioning the name of his pet on his social media account that he has revealed an answer to a security question that is commonly asked to recover one's passwords in case he forgets.[28]

[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] Alison Johansen, 11 ways to help protect yourself against cybercrime, Norton life lock, Sept.30, 2020.
[28] *Id.*

3. Beware of Identity theft

Identity theft takes place when one is tricked by fraudsters by means of deception. Often in cases of identity theft what happens is that an email is sent to a person with a view to trick him, in which person is asked to fill in his personal details like bank account number, by making him believe that he has won some prize so he needs to share credentials to avail benefits.[29]

4. Educating children

Teaching children about the way of using the internet in a manner that tends to make them use the internet more safely becomes quite crucial. For it is not a difficult task for criminals to decept children. Children are also required to be assured that they can at any time contact their parents in case they become a victim of online harassment or bullying.[30]

5. Data protection

One should make sure that whenever he deals with regards to financial records he uses them in encrypted form.[31]

6. Using strong passwords

It is very basic yet often ignored. Passwords should not be such as one can easily guess. They should not be related to the personal details of the individual. What else an individual can do is he can avail services of some reputed people who are in the business of password managing for the generation of some strong passwords.[32]

7. Contact forthwith

On being asked over a call from a company to reveal personal details one should immediately receive the company's contact details by visiting their official website and cross-check the fact.

However, one should call from a different device as till the time call is paced fraudsters might hold the line open and become conscious and pretend to be from that company.[33]

8. Being aware of URLs

One should be vigilant enough while clicking on any URL to see whether it looks like a genuine one. In case of even a bit of doubt on its legitimacy, it is better to avoid clicking on

[29] *Id.*

[30] 11 ways to protect yourself against cybercrime, cyber laws and information security advisors.

[31] *Id.*

[32] Tips on how to protect yourself against cybercrime, Kaspersky.

[33] *Id.*

that.[34]

V. Conclusion

Technological advancements which were intended to bolster the slow mechanism of the working process appear to have lead the country to a whole new trouble. With the rise in cybercrimes idea of cyberspace being used to get things done within a quick time seems to have taken a back step. While there were hardly a few crimes committed over cyberspace in its initial days it has led to such a situation where a large number of crimes are committed using the medium of technology. With the growing rate of crime what also makes the scenario worrisome is the potency of these crimes to affect a large population within a few seconds. Low-risk high return is the policy behind this surge. Low risk in a way that culprits while committing these crimes need not be physically present at the actual scene of crime reduces the possibility of them being caught to a great extent. Within a short period, there has been a rapid increase in crimes committed over the internet as has been shown in the report by National Crime Record Bureau (NCRB). This drastic change in the true purpose for which the internet was introduced demands a change in modus operandi of ours as well related to the way we use our gadgets. It is the time that we get more aware of DOs and Don't while working over cyberspace. It is not within an individual's control to prevent the commission of the crime. However, there are some precautionary steps as have been discussed in this write-up which should be taken by individuals in order to protect themselves from the cyber threat or least to say to minimize the quantum of damage which can be caused when their system is under cyber threat. By keeping a check on software updates every few weeks and by being a little vigilant while clicking on URLs or when sharing any sort of personal information over the internet people can to a great extent reduce the chances of succumbing to cyber attacks.

*****

[34] *Id.*