Page 1597 – 1616 **DOI:** *https://doij.org/10.10000/IJLMH.112414*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 6

2021

The Dark Side of the Internet: Cyber Crimes

SANCHIT MEENA[1] AND GAURI GIRDHAR[2]

ABSTRACT

The law of nature states that anything invented or discovered comes with its characteristics which involve both- the desirable and the undesirable goals which range from water to fire or two extreme vices. Having a desire to master the proficient side of any invention, people are also vehemently leaned towards learning the other- the bad aspect of the same. Internet was invented to assist the people but in present times we see that cyberspace is being misused vividly across the globe. According to Harvard University, cybercrime is an amorphous field and can be defined as any criminal activity that pertains to or is committed through the use of the Internet. All over the world, the notion of secure cyberspace has remained significant but has not been addressed properly due to its wide scope of accessibility. Crimes today are not just limited to the real world but have also emerged virtually with more and more forms of cybercrimes coming up these days as a result of the advancement in technology. The cases of victimization on the internet are elevating at a rapid speed because there is no coordination among the nations on the same issue at a global level. In the new normal, where most of the people are working from home, controlling cyberspace via effective laws remains an underrated topic because the main focus is controlling the spread of viruses along with boosting economic activities. In an ever-changing society, it is imperative to balance the right to the internet with other fundamental rights because nobody deserves to be a victim of cybercrime. This paper attempts to understand the nature of cybercrimes and also addresses the problems faced while reporting such forms of crimes. This research paper could help analyze the understandings of the youth concerning cybercrime as they are the ones who are most active on the platform of cyberspace. Further, this paper could help in measuring the effect of victimization of women on the internet and also the problem faced by them while reporting virtual crimes.

Keywords: Cybercrimes, Cyberspace, Lack of awareness, IT Act, Right to Privacy.

[1] Author is a Student at Symbiosis Law School, Pune, India.
[2] Author is a Student at Symbiosis Law School, Pune, India.

 [ISSN 2581-5369]

I. INTRODUCTION

The invention of ARPANET (Advanced Research Projects Agency Network) in the late 1960s and the creation of the World Wide Web by Tim Berners Lee in the 1990s made human lifemuch easier and in today's world internet remains one of the most powerful creations of man that offers people endless knowledge and entertainment to its users. From banking to research, shopping to entertainment, the internet has made it possible to communicate any piece of information to anyone, anywhere in the world in a fraction of seconds. Nowadays peoplecan also transmit or share information with a broad audience through social mediaplatforms, these platforms allow people to be more expressive and eloquent.

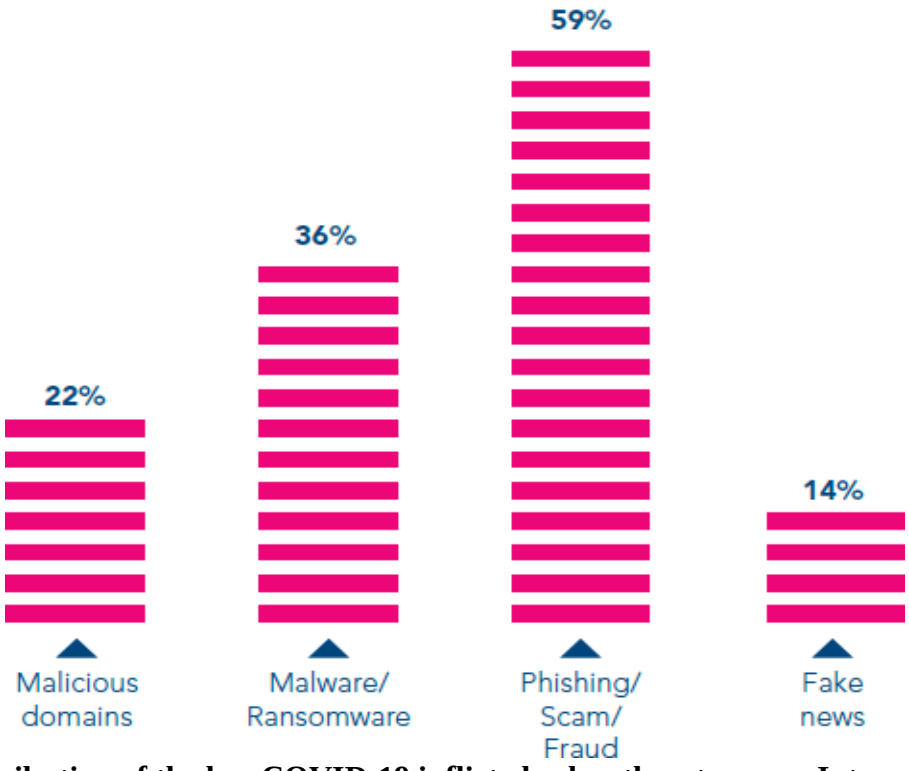
Life was different before the invention of the internet when Amazon was just a river, trolls were mythical creatures and pre-internet tinder dating was very different. Gradually as thehorizons of the internet and technology expanded, it started to offer diverse benefits for the ease and convenience of its users and now the internet covers every sphere of life ranging fromsecurity and defense to communication and learning. But as we all know that every coin has two sides, came the dark side of the internet where some of its users started experiencing cybercrimes or internet-based crimes.

According to Harvard University, cybercrime is an amorphous field and can be defined as 'any criminal activity that pertains to or iscommitted through the use of the Internet.' Cybercrimes are not new, the first person to befound guilty of the same was Ian Murphy in the year 1981 who hacked the American Telephone Company to manipulate its internal clock. Over time, cybercrimes started taking various forms such as Cyber Stalking, Cyber Bullying, Email Spoofing, Cyber Defamation, and many others. In the initial days of the internet, these types of activities were very rare as there were a small proportion of users, but gradually with timeas more and more people started using the internet the number of crimes multiplied which ledto the formation of various laws about the same in many countries. In 1996, the United Nations Commissions on International Trade Law rectified a model on Electronic Commerce which aimed to enable and facilitate commerce which was conducted using electronic means by providing national legislators with a set of internationally acceptable rules aimed at removing legal obstacles and increasing legal predictability for electronic commerce. In the year 2000, the government of India, keeping in mind the new developments, also enacted the Information and Technology Act, 2000 to deal with the cases of cybercrimes in our country and also became the 12th nation in the world to pass such legislation.

In the present times, the coronavirus pandemic struck the world at large, and to control the

 [ISSN 2581-5369]

virus, the government of many nations imposed nationwide lockdown where nobody was allowed to leave their homes. Therefore, during this period our phones, laptops, and tablets became our windows to the world, the internet was eventually used to its greatest potential with an increase in the number of users worldwide, and people no more had to leave their homes to socialize. As millions of people went online during this period for entertainment and more, total internet hits have surged between 50% - 70%, according to preliminary statistics. Streaming had also jumped by at least 12%. When the government wasoccupied to contain the spread of the virus, criminals were taking advantage of the increased security vulnerabilities arising from remote working to steal data, generate profits,and cause disruption. With the confinement of people in one place, there was an increase in the use of social networking apps. According to Interpol, phishing/ scam/ fraud increased by 59% in the pandemic. The following bar graph illustrates the increase in cyber threats in the lockdown period:



Distribution of the key COVID-19 inflicted cyber threats as per Interpol

As many people aren't aware of the proper use of cyberspace, they often end up being thevictims of online frauds and cybercrimes. It has also been observed that the victims of cybercrimes face difficulties in getting justice mainly because administration officials aren't trained enough to control these types of crime. In 2016, the United Nations declaredthe internet to be a human right, and specifically, an addition was made to Article 19 of the Universal Declaration of Human Rights (UDHR), which states: "Everyone has the rightto freedom of opinion and expression; this right includes freedom to hold opinions withoutinterference and to seek, receive

and impart information and ideas through any media andregardless of frontiers." Section 32 adds "The promotion, protection, and enjoyment of human rights on the Internet" and another 15 recommendations that cover the rights of those who work in and rely on internet access. In India, the Supreme Court too declared internet access a fundamental right by pointing the following:

A government cannotdeprive the citizens of fundamental rights except under certain conditions explicitlymentioned in the Constitution. The ruling came on hearing of a plea in connection with Internet blockade in Jammu and Kashmir in August 2019 -- in the view of revoking Article 370 in the Union Territory. Even though cyberspace offers many advantages, at thesame time it has the potential of being misused too. Thus, it is high time to put an end to cybercrimes and spread awareness about the prevailing laws, and also make people responsible for the proper use of cyberspace. In an ever-changing society, it is importantto balance the right to the internet with other fundamental rights.

Review of Literature

1. Porcedda (2014) directed towards balancing human development alongside cybersecurity. She pointed towards NCRB data release which stated an increase of 122.5% in crimes about cyberspace in the country of India in the year 2012. The research conducted by the author revealed that one of the main problems in regulating cybersecurityis the lack of international efforts due to regional and ideological differences, other problems such as lack of infrastructure and no training for curbing cybercrimes further worsen the problem. The paper concludes by suggesting some reforms to regulate cybersecurity at a global level despite all the differences in the legal system because thedevelopment of ordinary citizens is also hampered by an increase in cybercrimes.

2. Jeffray & Feakin (2015) highlight how almost all crimes have a technological component to them in the present world. The author also states that the usage of these exceptional technological weapons does not require any specialized expertise. The author shows that majority of cybercrimes are in pursuit of financial gain. It has helped us understand how jurisdictional issues hamper the investigation agencies to performing their respective duty anditalso analyses how crimes that originated in foreign jurisdictions hamper securing and analyzingthe evidence.

3. Rao (2016) focuses on how the privacy of an individual and human rights violation is at a stakewith the recent amendments in cyberspace. He presents how cyberspace can be used and misused. This research paper elaborates on the various cybercrimes and how various cyber laws

and legislations including Intellectual Property Rights (1999) deals with them. Rao presents the punishment for various offenses and makes us understand the need for awareness, the role of the human resource department, and the need to create a secure cyber ecosystem for the people.

4. **M. McKenzie** (2017) focuses on theft or exploitation of data; denial of access or service that affects the availability of networks, information. He also focused on destructive actions including corruption, manipulation, or activity that threatens to destroy the networks system. Cyber deterrence is a difficult strategy to achieve because there are many obstacles in placesuch as problems in attribution, the diminishing capability to retaliate, unnecessary escalation, involvement of non-state actors as well as the potential legal issues, making cyber deterrencean unviable strategy in practice.

5. **Holt** (2017) in the research found out that cybercrime has not confined itself only to the individual but has also developed to different institutions engaged in buying, selling, and trading our personal information. He pointed towards the use of data from the online cybercrimes market may serve as a vital source to understand the link between hacking and profits within the underground economy. It can be concluded that increased clarity in reporting of such crimes is vital to move criminological research beyond speculation for improving the current situation.

6. **Uma** (2017) scrutinized the most frequent forms of cybercrimes against women and also spotlighted landmark cases and judgments on the same. She directed towards the anonymity offered by the internet to culprits which also proves to be a barrier in the prevention and detectionof these crimes. She directed towards the Information and Technology Act, 2000 which offers separate legal provisions to control cybercrimes such as section 66A and 67A to particularly cope with internet-related offenses and certain provisions in the Indian Penal Code which provides remedies in such offenses. This research paper has helped us to understandthat none of the existing laws fully address the situation of women in cyberspace. The needof the hour is to amend these laws considering the new circumstances and at the same timegenerate awareness about the proper use of cyberspace.

7. **Pawar & Sakure** (2019) shows with the help of statistics how the number of internet usersis directly proportional to the number of crimes coming up these days and throws light on how social media stimulates cyber-crimes. Further, they mention the present laws and highlight how they are not enough to combat the issue. The research paper is concluded bylisting a few measures which may help in controlling cybercrimes to some extent shortly.

8. Barker & Jurasaz (2019) scrutinize women and their everyday experiences of violence, harassment, and political struggle and how these acts severely affect women's rights to equalparticipation in the public sphere. They also focus on how recent studies have shown that significant percentages of women and girls have faced abuse online, especially on social media, with the vast majority of such abuse motivated by sex and gender discrimination. Thus, there is no exception to women who have been criticized from Diane Abbott to Sushma Swaraj, it can be interpreted that the critics do not know any limits. Therefore, according to the authors, online platforms are not restricting information, but are accountable actors from the perspective of international law, which means that they must take responsibility for the content that is posted and shared within their platforms.

9. Devi & Kumar (2020) addresses the concern of cybercrimes against women. The utmost reasons for easy victimization are gender distinction, the fright of defamation in a community,lack of awareness, and no existing proper legislation to address the problem of cyber-attackson women. Lack of assistance on the part of the police and the administrative officials is one of many reasons behind not reporting such types of crimes. They have pointed towards facing difficulties of victims not only in focusing on their careers but also in living a peaceful life in society after reporting such crimes. The paper concludes by suggesting ways to combat cybercrimes by emphasizing strong laws and the regulation of preventive tools in cyberspace.

10. Vasiu[1] & Vasiu[2] (2020) portray the current scenario where crime and technology are expanding their ambit. On one hand, technology is helping people in gathering profound knowledge, on the other hand, it is distorting people's lives. The author also explains how the scale, scope, and challenges posed by these criminal phenomena cannot be overstated. The author illustrates how police officers, law officers, and even judges have threatened through mails and other mediums by naming a few cases. The author winds up by suggestingthe measures such as awareness, education, law enforcement, increased reporting of such cases to tackle cybercrime.

11. Decker, Rauhut & Fabro (2020) talks about the pernicious effects of cybercrime particularly in the nuclear sector. They stressed the threat that cybercrimes possess whiledealing with nuclear radiation in today's world. They also discuss the malicious intent ofcriminal-minded people who posed a threat to society in a world when hacking and othercyber offenses are increasing. They also take into consideration the work of different agencies such as the world institute for nuclear security, the internet security alliance, and the international atomic energy agency among others towards achieving a threat-free society. The collaborations can be through a new international organization or a network ofcooperating States, private sector

 [ISSN 2581-5369]

cyber specialists/organizations, universities, and/or individuals to work hand in hand. This research paper has helped us to understand that prioritization is key for controlling virtual crimes.

II. ACT RESPONSIBLE FOR REGULATING CYBERCRIMES

Information and Technology Act (IT ACT), 2000

The Information and Technology Act, 2000 (IT ACT) is the backbone for governing cybercrimes in India. It is perhaps the only act in India that is completely devoted to the offenses prevailing on the platform of the internet. Section 66 of the IT act prescribes the punishment for internet-related offenses, mentioned in section 43 of the same act. Various subєlauses of section 66 further deal with other forms of cybercrimes such as identity theft, cyberterrorism, violation of privacy, and others. In the case of *Shreya Singhal v Union of India (2015)*, section 66A of the IT Act was discarded as unconstitutional on the ground of being incapable of the morals laid by the constitution, but we see that despite this revocation it isstill being used all over the country to arrest the accused in crimes about cyberspace. This points towards an effective system of increasing awareness among police officials regarding the decimalization of Section 66A.

Section 67 further deals with the offense of propagating indecent material on the internet, it also highlights the punishment for such an offense, this section subsequently deals with the crimeof child pornography and disseminating sexually explicit content via the internet. Section 72 throws light on the penalty for the violation of confidentiality and privacy. Section 84 B and84 C respectively discuss abetment and attempt of all the offenses mentioned in the IT Act, 2000. In the year 2008, the IT Act was amended considering new circumstances which arose over the years, and new sub-clauses were added. (IT ACT, 2000). Whereas on the otherhand, in cases of virtual crimes where women are a victim, different provisions of IPC are used along with IT Act to arrest the accused.

DIFFERENT TYPES OF CYBERCRIMES

CRIME	DEFINITIONS	PUNISHMENT
Cyber Defamation	Publishing of false statement about an individual in cyberspace.	Imprisonment up to 2-3 years or fine or both.

Cyber Stalking	The repeated use of the internet to harass or frightensomeone.	Imprisonment up to 5years and fine of 1lakh OR fine of Rs 2lakh with 2years of imprisonment.
Cyber Bullying	The use of electronic communication to bully aperson.	Imprisonment for 1-2years and fine depending upon the section applied.
Cyber Blackmailing	The act of threatening to share information about a person to the public via the internet.	Imprisonment of 7years or fine or both.
Scam/Fraud	A fake scheme for stealing money or goods.	Imprisonment of 6months-10 years and fines which may extend to 3times of the fraudulent amount.
Fake News	Misinformation spread *via* print, media, or online formssuch as social media.	Imprisonment can extend up to 3 years or fine or both.
Malicious Domains	Tools providing the hierarchy of unique identifierswhich guide traffic across the world web and identify other resources. It is also the basic tool in the hands of criminals.	Imprisonment up to 3 years or fine up to 5lakhs or both depending upon sections.
Morphing	To change from one image to another using computeranimation techniques.	Imprisonment up to 2years and fine of Rs 2000 OR Imprisonment of 5years and fine of Rs 5000 in subsequent conviction.
Email Spoofing	The forgery of an email sender addresses so that the	3 years imprisonment and a fine up to Rs 2lakhs.

 [ISSN 2581-5369]

	message appears to have come from some other source than the actual source.	
Sending Obscene	Sending obscene pictures/messages.	Imprisonment of either description for a term which may extend to 3 months, or fine or both.

III. RESEARCH METHODOLOGY

Objectives of the Study

1. To understand the concept of cyber-crime.
2. To understand the difficulties faced while reporting cyber-crimes.
3. To find out the awareness of cybercrimes and cyber laws amongst the masses.
4. To suggest the measures to tackle cyber-crimes.

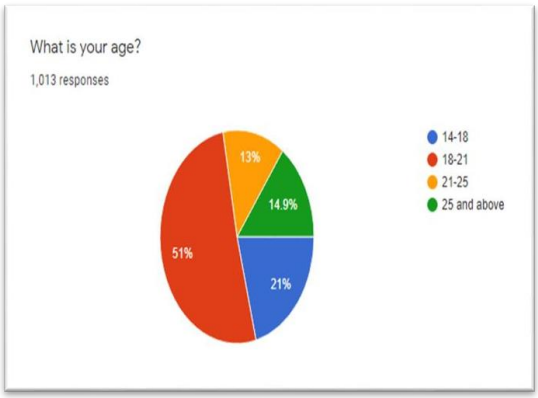
Research Method

The sources of research are based on both Primary and Secondary data. The Primary Data hasbeen collected *via an* online survey which was conducted via Google forms from '1013'respondents which consisted of people of age group "14-18", "18-21", "21-25" and "25 & above". This questionnaire was distributed *via the* internet randomly and contains responses frompeople residing all over the country. Secondary data is also used in the research and has beencollected through numerous Journals, Articles, Reports, Research Papers, and Books about the same topic available online. The findings from the sample were theninterpreted thoroughly and have been generalized to a bigger crowd falling in the same age group.

 [ISSN 2581-5369]

IV. FINDINGS AND DISCUSSIONS

Findings



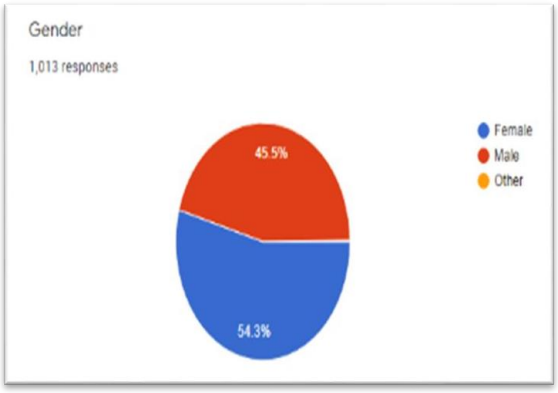
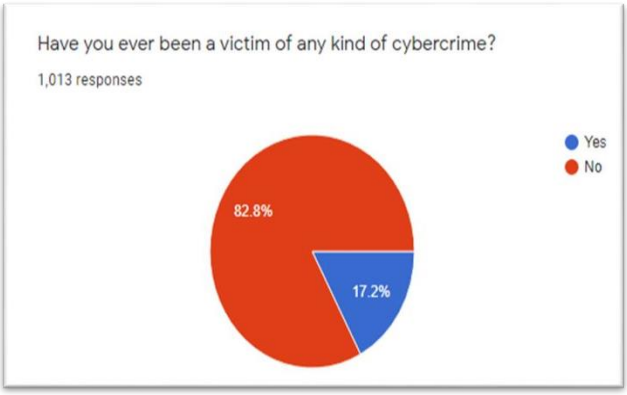


Figure 1 Figure 2

Figure 1 says, out of 1013 people surveyed, the 14-18 age group was 21%, 18-21 was 51%, 21-25 was 13% and 21% being respondents above 25 years of age.

Figure 2 shows that, out of 1031 people surveyed, 45.5% were Male, 54.3% Female while 0.2% others.

Figure 3 Figure 4



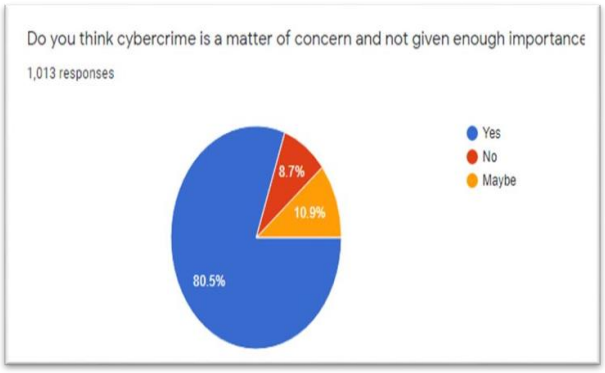


Figure 3 shows that out of the total number of people surveyed, 17.2% people have been a victim of cybercrime while 82.8% have not.

Figure 4 shows that out of the total number of people surveyed, 80.5% think cyber-crime is a matter of concern while, 8.7% do not think so and 10.9% are not aware of the same.

Figure 5 Figure 6

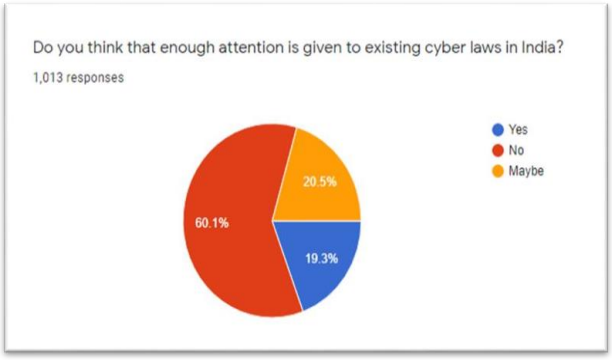
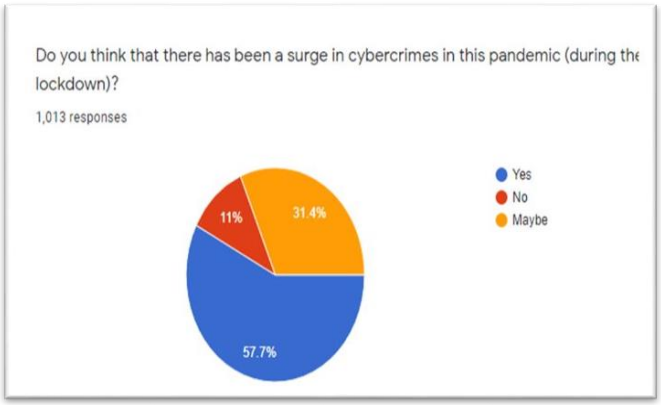


Figure 5 shows that out of the total number of people surveyed, 52.2% think that the legal system of our country does not provide appropriate provisions for tackling cybercrime while 26.7% does not think and 23.1% are not aware of the same.

Figure 6 shows that out of a total number of people surveyed, 60.1% do not think that enough attention is given to the existing cyber laws in India while just 19.3% think so, 20.5% are not aware of the same.so,

Figure 7 Figure 8



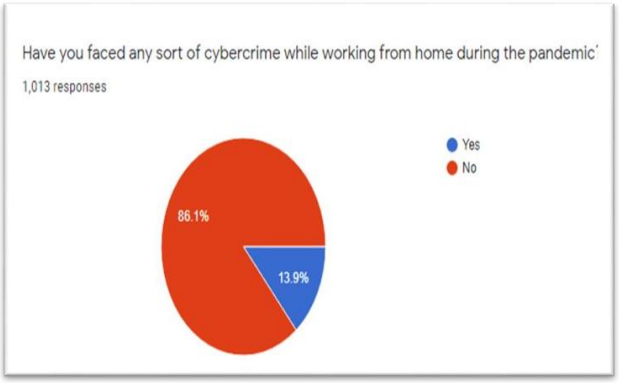
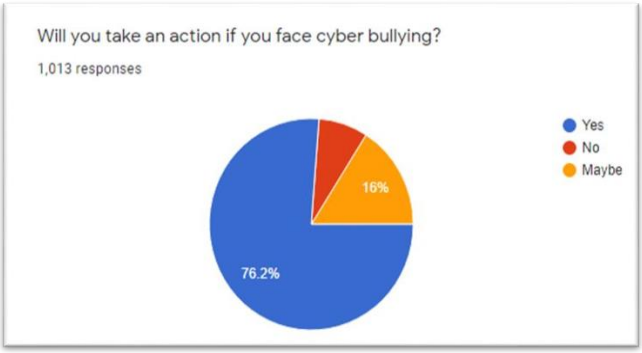


Figure 7 shows that out of the total number of people surveyed, 57.7% think that there has been a surge in cybercrimes during the Pandemic, whereas 11% do not think so, while, 31.4% are not aware of it.

Figure 8 shows that out of the total number of people surveyed, 13.9% faced cybercrime while working from home, while, 86.1% did not.

Figure 9 Figure 10



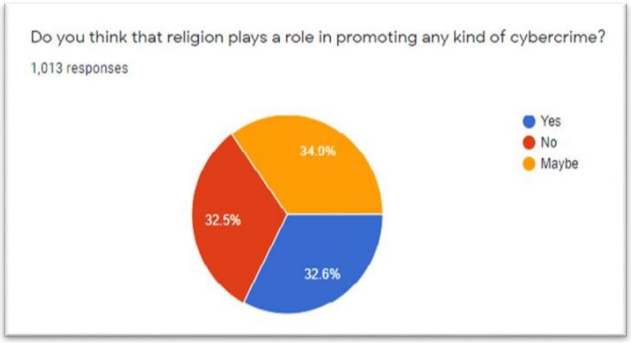
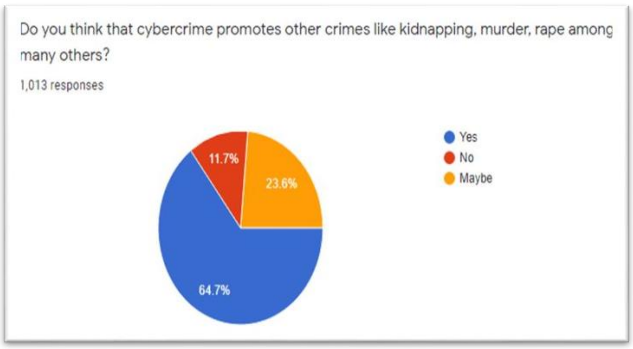


Figure 9 shows that out of the total number of people surveyed, 76.2% people are willing to take action if they face any sort of cybercrime while 7.8% are not, 16% are not sure about the same.

Figure 10 shows that out of the total people surveyed, 32.6% people think that religion plays a role in promoting cybercrime while 32.5% do not think so and 34.9% are not aware of it.

Figure 11 Figure 12



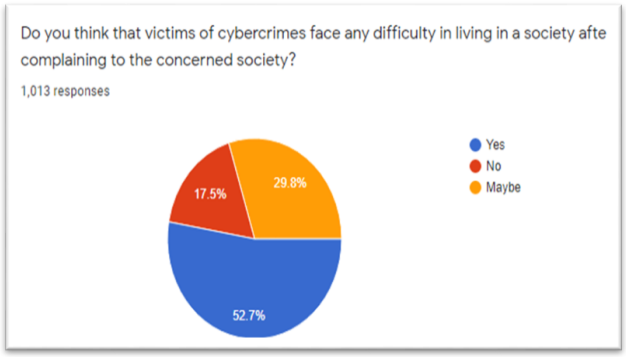
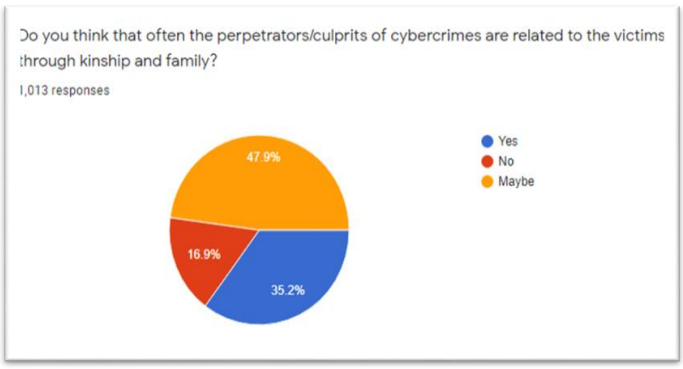


Figure 11 shows that out of the total number of people surveyed, 64.7% think that cybercrime promotes other crimes whereas 11.7% do not, while, 23.6% are not aware of the same.

Figure 12 shows that out of the total number of people surveyed, 52.7% think that the victims of cybercrimes face the difficulties in living safely in the society while 17.5% do not think so and 28.9% are not aware.

Figure 13 Figure 14



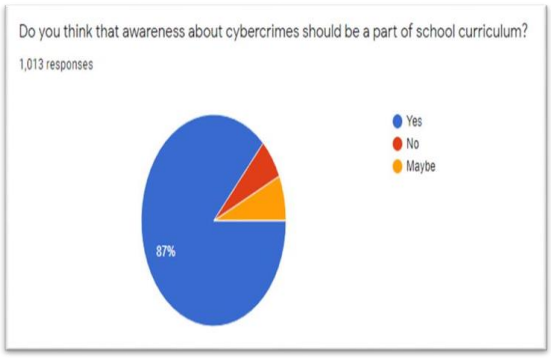


Figure 13 shows that out of the total number of people surveyed, 35.2% think often culprits of cybercrime are related to the victims and family while 16.9% do not think so, and 47.9% are not sure about it.

Figure 14 shows that out of the total number of people, majority of them i.e., 87% think that the awareness about cyber laws should be a part of School curriculum while a few

ATA ANALYSIS AND INTERPRETATION

The above pie charts show the consolidated graphical presentation of the responses collected *via* Google forms. Since the research was focused on analyzing the perspective of different age groups towards cybercrimes and the current notion of dealing with cybercrimes, the questions were based around the issue.

The research dealt with four different age groups, i.e. “14-18”, “18-21”, “21-25” and “25 and above, 45.5% of which were males and 54.3% females and 0.2% others which clearly shows thatmost of our respondents were females. To start with, 17.2% of the respondents have faced somesort of cybercrime. Surprisingly, from our research, we found out that 80.5% of the total respondents think that cybercrime being a matter of concern is not given enough attention in ourcountry. While 50.2% of respondents think that the legal system of our country does not provide appropriate provisions to tackle cybercrimes and the administrative officials are not trained enough to handle such crimes, but, 26.7% do not think so and 23.1% don’t know which depicts the lack of knowledge among people. The pandemic has deteriorated the condition as 57.7% of the respondents think that there has been a surge in cybercrimes during the pandemic while a majority of them i.e. 31.4% do not know about the same. It was also analyzedthat 13.9% of respondents were the victims of cybercrime while working from home during the pandemic.

The best part of this is that 76.2% of people are willing to report and take an action if they face any sort of cybercrime, a few of them i.e. 4.8% are not while 16% are not sure about it.But, with awareness, more people will be motivated to take any action to tackle cybercrime. The one question on which people didn't show any specific response was related to whether religion plays any role in cybercrime. The responses were very close as 32.6% think it does while 32.5% don't think the same way and the remaining are not sure about it. Surprisingly, 64.7% of the respondents think cybercrime promotes other crimes too. 52.7% think that victims of cybercrimesface difficulties living in society while 17.5% do not think so. The respondents were not surewhether the culprits were related to the victims as 36.2% think so while a majority of them i.e. 47.9% are not aware of the same and 16.9% do not think so. The best part is that 87% think awareness should be a part of the school curriculum.

It can be interpreted that there is a need to make people aware of the existing laws andways to prevent them from cyberattacks. They should also be taught how to use the internet safely. The need of the hour is to encourage people to come up and report cybercrimes if they face any.At the same time, it is very important to educate and train the officials and make them aware of existing laws. Amendments should be brought in the law where necessary and new legislation should be passed to tackle the rapid growth of cyberattacks. The victims many a timeface difficulty in coping up with society, thus, people should be taught how to offer a helpinghand rather than creating more problems for them. And finally, awareness should become a part of the school curriculum which will teach the children how to use the internet properly while embedding the value of respecting each other on cyberspace at a primary level.

V. CONCLUSION

Saumya Uma once quoted that "if the religion was the opium of masses in the past, social media has become a new opium as well as the tsunami of India today." Internet was created with a good intention to provide a platform that was accessible to everyone despite the differences prevailing in the world but with current trends of an increase in cybercrimes, we comeacross the fact that it is not secured if one is not taking mandatory precautions at a local level from his/her side. After conducting this research, we concluded that even though the issue of cybercrimes is very crucial considering the usage and potential of the World Wide Web, we see thatthis issue remains as something less important in the 21st century which is because of lack of awareness among the masses. Virtual crimes are the crimes committed on the platform of cyberspace by various soft wares and techniques but also remain unaddressed due to the lack ofsupport available.

 [ISSN 2581-5369]

According to our analysis of primary data, we concluded that most people have just a mereidea about the whole issue of cybercrimes and there is very little or no proper knowledge about the same. Keeping our objectives of the research study in mind, it can be interpreted that the whole concept of cybercrime is certainly overlooked because no support is available from the government to curb the same. Due to this lack of awareness, the reporting of such forms of crimes has remained less because the state officials aren't equipped enough to probe into the matter unlike remedies available to curb other forms of wrongs prevailing in the society. Even though we have exclusive legislation in place that is the IT Act of 2000, it is not enough and competentto deal with all forms of cybercrimes after a scrap of section 66A of the same by the honorable Supreme Court of India. It is important to understand that despite this scrapping, the same section is still widely used all over the country, the need of the hour is to address the issue properly by working and coordinating with various stakeholders in the IT sector for better implementation of laws and policies. At a holistic level, this can be achieved if everyone in the nation starts considering cybercrimes alike all crime and not as something which is still in the process of evolving.

RECOMMENDATIONS

After conducting the research, we got to know that section 66(A) of the Information and Technology Act has been scrapped and there are no new amendments in the cyber laws recently. As a result of advancements in the field of the internet, different types of cybercrimes are being witnessed and the number of victims is also rising. Thus, the need is to make new and strict lawsor amendments to the existing ones. Apart from it, the different age groups should be made aware of the different types of cybercrimes and the existing cyber laws. They should also be taught why it is important to keep confidential information like ATM PINs, Passwords, and OTPs to only themselves. Along with it, parents should keep a check on every online activity oftheir children in a friendly way. The IT Industry also possesses a great scope as it may develop software that automatically filters the threat or make the user aware of the potential threat of any activity in cyberspace.

VI. LIMITATIONS AND FUTURE SCOPE

In our research, the biggest limitation was posed by covid-19 as the Pandemic restricted the research to a great extent, resulting in which, there was no personal interaction and physical collection of samples. The random samples were collected online *via* Google Forms and we were unable to interact with the respondents physically. Time played a role in limiting our research andas a result of this, a smaller number of research papers and journals have been referred.

 [ISSN 2581-5369]

Future researchers can explore the rate of cybercrimes in rural areas as a large population of internet users belong to rural areas. Future researchers may target a definite age group of 14-19 years i.e. teenagers to study the impact and influence of the internet on young minds. Researchers may also consider the aspect of awareness in two parts i.e., awareness among theofficials/authorities concerned and the awareness of common people in general. The need of thehour for our country is employment, therefore, research on the probable employment opportunities in the field of cybersecurity engineers is an aspect to be considered. The in-depth studyon cyber-attacks related to the financial aspect offers a field of scope too as cybercrimes in this sectorare elevating at an alarming rate.

*****

 [ISSN 2581-5369]

VII. BIBLIOGRAPHY

- Barker, K., & Jurasz, O. (2019). Online misogyny: a challenge for digital feminism. *Journal of International Affairs, 72*(2), 95-114. Retrieved from https://www.jstor.org/stable/26760834
- DECKER, D., RAUHUT, K., & FABRO, M. (2020). Prioritizing actions for managing cybersecurity risks. *StimsonCenter*. Retrieved from www.jstor.org/stable/resrep25113.
- Devi, P., & Kumar, S. (2019). A Discourse on Cyber Crime against Women: Problems and Prospects. *Precedent: A Publication of Jus Dicere & Co,* 3(1), 1447-1469. Retrieved from https://www.jusdicere.in/a-discourse-on-cyber-crime-against-women-problems-and-prospects/
- Fatima T. (2016). *Cyber Crimes (2nd Ed.)*. Lucknow, India: Ebc Publishing (P) Ltd.
- Holt, T. (2017). Cyberinfrastructure protection. *Strategic Studies Institute, US Army War College*. 3(pp. 35-62, Rep.) (Saadawi T. & Colwell J., Eds.). Retrieved from https://www.jstor.org/stable/resrep11978.6
- Jeffray, C., & Feakin, T. (2015). Underground Web: The Cybercrime Challenge. *Australian Strategic Policy Institute*. https://www.jstor.org/stable/resrep04074?seq=1#metadata_info_tab_contents
- Rao, K., (2016). Human rights and cyberspace: use and misuse. *Bharti Law Review. July-Sept.* 5-31. Retrievedfrom http://docs.manupatra.in/newsline/articles/Upload/C4971E8F-86E8-48E1-886B-CEF0B774397F.pdf
- McKenzie, T. (2017). Challenges of cyber deterrence. *Air University Press*. Retrieved from https://www.jstor.org/stable/resrep13817
- Pawar, M., & Sakure, A., (2019). Cyberspace and Women: A Research. *International Journal of Engineering and Advanced Technology (IJEAT),* 8 (6S3). Retrieved from https://www.ijeat.org/wp-content/uploads/papers/v8i6S3/F13130986S319.pdf
- Porcedda, M. (2014). Riding the digital wave: The impact of cyber capacity building on human development. *EuropeanUnion Institute for Security Studies (EUISS).* (pp. 28-42, Rep.) (Pawlak P., Ed.) Retrieved from https://www.jstor.org/stable/resrep07069.7?seq=1#metadata_info_tab_contents
- Uma, S. (2017). Outlawing cyber-crimes against women in India. *Bharti Law Review. April-June. 103-116.* Retrieved from https://docs.manupatra.in/newsline/articles/Upload/CE3E0AE8-DE2B-41EA-92A2-8A46035DECEB.pdf

- Vasiu, I., Vasiu, l. (2020). Forms and consequences of the cyber threats and extortion phenomenon. *European Journal of Sustainable Development. 9(4). 295-302.* Retrieved from http://ecsdev.org/ojs/index.php/ejsd/article/view/1141
- Beech, M., (2020, May 25) *COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal.* Retrieved from https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=12213fc43104
- *Cybercrime: Covid-19 Impact.* (n.d.). Retrieved from https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats

VIII. APPENDIX

Questionnaire (tick the suitable option)

1. What is your age?
    - 14-18
    - 18-21
    - 21-25
    - 25 and above
2. Gender
    - Male
    - Female
    - Other
3. Have you ever been a victim of any kind of cybercrime?
    - Yes
    - No
4. Do you think cybercrime is a matter of concern and not given enough importance?
    - Yes
    - No
    - Maybe

5. Do you think the legal system of our country provides appropriate provisions for tackling cybercrimes andthe administrative officials are trained enough to handle such crimes?
    - Yes
    - No
    - Maybe
6. Do you think that enough attention is given to existing cyber laws in India?
    - Yes
    - No
    - Maybe
7. Do you think that there has been a surge in cybercrimes in this pandemic (during the lockdown)?
    - Yes
    - No
    - Maybe
8. Have you faced any sort of cybercrime while working from home during the pandemic?
    - Yes
    - No
9. Will you take an action if you face cyberbullying?
    - Yes
    - No
    - Maybe
10. Do you think that religion plays a role in promoting any kind of cybercrime?
    - Yes
    - No
    - Maybe
11. Do you think that cybercrime promotes other crimes like kidnapping, murder, rape

 [ISSN 2581-5369]

among many others?

- Yes
- No
- Maybe

12. Do you think that victims of cybercrimes face any difficulty in living in society after complaining to theconcerned society?
    - Yes
    - No
    - Maybe
13. Do you think that often the perpetrators/culprits of cybercrimes are related to the victims through kinshipand family?
    - Yes
    - No
    - Maybe
14. Do you think that awareness about cybercrimes should be a part of the school curriculum?
    - Yes
    - No
    - Maybe

*****