Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Victimization of Females in Cyberspace - A Study on Females enrolled in Higher Education Institutions in India

Dr. Sheetal Arora[a] Poonam Yadav[b]

[a]Assistant Professor, Department of Criminology and Police Studies, Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, India [b]Sardar Patel University of Police, Security and Criminal Justice, Jodhpur, India

Received 20 February 2022; *Accepted* 11 March 2022; *Published* 14 March 2022

Cybercrimes against females are one of the fastest-growing problems in our society. Since there is an increase in digitalization across the world, the number of internet users increases daily. Most of the users are unaware of the advantages and disadvantages of using the Internet. As a result, one may observe an immense rise in cybercrimes against females. Cyberspace is equally open for perpetrators without any boundaries. Here, perpetrators are active in exploiting the vulnerable females while they explore themselves virtually. Cybercrime has emerged as the biggest threat to the privacy of people and a crucial challenge for Law Enforcement Agencies despite exiguous attention from legislators and researchers. "India has failed in getting the requisite convictions in cybercrime cases the number of such crimes is rising," says cyber law expert and Supreme Court advocate Pavan Duggal (Masoodi, 2016)[1]. This research paper explores the present scenario regarding incidences of cybercrimes against female students from an Indian perspective. The findings of this study include information about the reasons for cyber victimization, cybercrime trends, and the status of reporting to the agencies from the victims' perspective. The first-hand data is collected using the non-probability sampling method from 200 respondents in online mode. The study provides two models, first on the reasons

[1] Ashwaq Masoodi, 'For victims of cyber stalking, justice is elusive' (*Live Mint, 26 July 2020)* <https://www.livemint.com/Politics/St93190XdGvpiclGWwnX0I/For-victims-of-cyber-stalking-justice-is-elusive.html> accessed 01 February 2022

for victimization and second on the motives of perpetrators behind Cybercrime based on the responses received. Lastly, it also suggests practical solutions and suggestions about cybercrime prevention strategies from an Indian perspective.

Keywords: *cybercrime, victims, cyberspace, social networking sites (SNSS), internet.*

INTRODUCTION

Any aim towards controlling cybercrimes requires deep insight and understanding into the elements contributing to this crime. Lately, research in the area of Criminology and Criminal Justice has made victims the focus. The victim in any crime including cybercrime is crucial in understanding the nature and intricacies of that crime. The present problem of crimes against females in cyberspace requires a search for many relating aspects. The increasing usage of the web and technology in daily routine and thereby increased opportunities for offenders for exploitation requires an urgent intervention to come up with measures to control the menace of cybercrime. Also, the damage to the victims is of varied nature since the event of occurrence is in cyberspace, which requires in-depth knowledge about this problem. Hence the present paper entails crucial aspects like the nature and prevalence of cybercrime against females, reasons for victimization in cyberspace from the victims' perspective, and characteristics of cybercrime against females.

CONCEPTUAL FRAMEWORK

Meaning of Victimization: It refers to an event where persons, communities, and institutions are damaged or injured in a significant way. Those persons who are impacted by persons or events suffer a violation of rights or significant disruption of their well-being[2]. Sellin & Wolfgang (1964) identified levels of victim impact as Primary Victimization, Secondary victimization, and Tertiary victimization.

[2] Joan P.J. Dussich, 'Victimology--Past, Present and Future' (2006) 70 Resource Material Series, 116-129 <https://www.ojp.gov/ncjrs/virtual-library/abstracts/victimology-past-present-and-future-resource-material-series-no-70> accessed 01 February 2022

Primary Victimization: Primary victimization occurs with the person who suffers directly by crime i.e. Rape victim, Cybercrime victim, Acid attack victim.

Secondary Victimization: Secondary Victimization includes the suffering of the individuals due to the suffering of direct victims' including their parents, children, and relatives.

Tertiary Victimization: Tertiary Victimization includes experiencing mental trauma by a larger population due to witnessing a serious form of victimisation. E.g. the whole nation stands together in the case of the Nirbhaya gang-rape victim for justice.

Victim: Section 2 of the Code of Criminal Procedure, 1973 defines the word 'Victim' as a person who has suffered any loss or injury caused by reason of the act or omission for which the accused person has been charged and the expression "victim" includes his or her guardian or legal heir;'[3]

VICTIMIZATION OF FEMALES

Victimization of females is not an unknown problem but with the passage of time, it increasingly gained the attention of lawmakers, judiciary and police, etc., Unfortunately, it's still a bitter truth of our society, that even now, females are victimized through various ways such as gender-based discrimination, child marriage, dowry death, sexual harassment, rape, etc. It is difficult to know, the actual rate of female victimization in several parts of India, especially in events like ragging, sexual harassment, gang rape, cruelty, witchcraft, cybercrime, etc that largely go unreported. The reason behind this is maybe the silence of this gender due to many unknown reasons, against such forms of victimization which leads to less reporting of such cases to the police. Often, the cases that are reported in the media press are generally the ones that the police are aware of. So there is a higher chance of the possibility of the presence of dark figures, which are unreported cases of this nature in India. Thus, one needs to research well to know the reality relating to the victimisation of females in our country.

[3] Code of Criminal Procedure, 1973, s 2

VICTIMIZATION AGAINST FEMALES FROM PHYSICAL SPACE TO CYBERSPACE

Due to the rapid increase in digitalisation, there is a shifting of places of criminal incidences from physical space to cyberspace. Criminal incidences in cyberspaces have now been reported, like Cyber sexual harassment, stalking Cyberstalking, etc and in cyberspace, the perpetrator can easily hide their identity and can commit any crime from sitting in one country and committing crimes in another county.

VICTIMIZATION OF FEMALES IN CYBERSPACE

India was ranked second among the countries with the most internet users in 2019[4]. The number of internet users increases in both urban as well as rural areas, showing a rapid growth in access to the internet, which also leads to the hike in Cybercrime. Cybercrime is a global phenomenon with an ample opportunity of maintaining the anonymity of perpetrators and flows easily around the world without any physical boundary. As every coin has two faces, the internet also has its two sides one, it empowers females by providing the opportunity to work from home, easy communication with the whole world, and on the other side, it leads to the victimization of people especially females on the digital platform.

Today youth are more curious to know about the global phenomenon so they spend more time daily on the Internet to gain information and to connect with friends through SNSs. Perpetrators use this digital technology to harass and abuse females in Cyberspace by accessing personal information through hacking, stalking, etc., even though these cyber crimes against females have not been given the kind of priority in India as these deserve, these crimes are perceived as minor crimes with lenient punishment. Delhi-based clinical psychologist Pulkit Sharma says, "When someone harasses you online, it is viewed by a much larger audience and you feel helpless about not being able to contain the spread of that false information or a photograph. So, the sense of shame, the trauma, the feeling of being exposed,

[4] Joseph Johnson, 'Countries with the highest number of internet users as of June 2019' (*Statista,* 31 January 2022) <https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/> accessed 01 February 2022

is much, much higher.[5]" (Masoodi, 2016) As India is also one of the few countries to enact the IT act 2000[6] to combat Cybercrime it is mostly confined to e-commerce or economic offenses in which most of the offence is bailable and not fully covered the offences against people. The Act turned out to be a half-baked law as the operating area of the law stretched Cyber Victimization of Women and Cyber Laws in India[7] (Jain, 2017) This present study is an attempt to find out the prevalence in terms of dark figures of Victimisation of Female Students in Cyberspace among Higher Education Institutions. Although it's very difficult to stop Cybercrime completely, this study is an attempt to find the trend of cybercrime, reasons for victimization and aims to suggest measures for preventing the victimisation of female students in Cyberspace so they can safely surf on the internet and communicate with friends on SNSs without any fear.

CYBER HARASSMENT

Cyber harassment (online harassment): Cyber harassment is the use of email, instant messaging, and websites to bully or harass an individual through personal attacks. Cyber harassment can be in the form of comments made in chat rooms, sending offensive e-mails, or even harassing others by posting on social networking sites[8]. According to stats published by Sanika Diwanji on Statista states that in 2018 alone, India recorded over two thousand cases of cyber crimes related to sexual harassment and over 700 cases of cyberbullying against women and minors. In 2018 over 2000 cases of cybercrime related to cyber-harassment or exploitation were reported... This was a stark jump in the number of such cyber crimes in the country compared to the previous two years. Woman's harassment and exploitation in cyberspace are increasing with updated technology and anonymity. It takes a huge time for investigation and many times cases are unsolved due to the lack of Cyber Forensics laboratories.

---

[5] Ashwaq Masoodi (n 1)
[6] Information and Technology Act, 2000
[7] Dr. Monika Jain, 'Victimization of women beneath cyberspace in indian upbringing' (*Manupatra Doc,* 5 May 2020) <http://docs.manupatra.in/newsline/articles/Upload/786274E9-B397-4610-8912-28D6D03230F9.monika_jain_pdf_1-1111.pdf> accessed 02 February 2022
[8] 'Cyber Harassment Law and Legal Definition' (*US Legal*) <https://definitions.uslegal.com/c/cyber-harassment/> accessed 02 February 2022

CYBER STALKING

Stalking is the behavior wherein an individual willfully and repeatedly engages in a knowing course of harassing conduct directed at another person which reasonably and seriously alarms, torments, or terrorizes (create fear) that person. Stalking on the internet happens when the perpetrator follows the victim continuously by leaving unwanted messages. Most of the cases are reported where the target of cyberstalking is women, especially of the age group of 16 to 35. According to the **NCRB report**, in **2017** the number of 555 cases of cyberstalking and cyberbullying of women have been registered across India, with Maharashtra registering the most number of cases — 301 — among the states. Andhra Pradesh, with 48 cases, was second, and 27 cases were reported from Telangana and Haryana each, putting them in third place (**Staff, 2019**) Tatiana Begotti and Daniela Acquadro Maran conducted the study of over 250 students at the University of Torino. And found that about half of the participants experienced at least one incident of Cyberstalking. Among them, more than half experienced more than one type of Cyberstalking. Victims suffered from depression more than those who had never experienced Cyberstalking. Out of the participants, 65 (28.4%) indicated having suffered Cyberstalking through online contacts. Most of the victims were females (73.4%) and, for most of them, the stalker was a man (73.5%). He was a friend or acquaintance in 53.8% of the cases and a partner or ex-partner (20%) or a stranger (26.2%) in the remaining cases. For 24 subjects (85.9%), the stalking behavior using online contact had already ended.

IDENTITY THEFT

According to an article published in the year 2018, the southern state of Karnataka in India had the highest number of registered offenses related to online identity theft, with more than 5,000 cases registered with the authorities. The country recorded approximately 6,700 cases of online identity theft that year. This category of crime came under the purview of Section 66C of the Indian Penal Code[9]. There has been an alarming spurt in cases of identity theft — stealing someone's details to access resources or obtain credit or other benefits in that person's name or

[9] Sandhya Keelery, 'Number of online identity theft offences reported across India in 2018, by leading state' (*Statista*, 19 October 2021) <https://www.statista.com/statistics/1097526/india-number-of-online-identity-theft-offences-registered-by-leading-state/> accessed 03 February 2022

misusing the victim's details for nefarious purposes. In most cases, conmen access the accounts of individuals on various social networking sites such as Facebook, Twitter and retrieve their photos and other information and misuse the same for different purposes. Inspector Suresh Singh, Cyber Crime Cell in-charge, said, "Victims often withdraw their complaints as most of the accused are known ones. Many students do not realise when they use webcams to interact with their friends who often record the videos."

CYBER PORNOGRAPHY (REVENGE PORNOGRAPHY AND NON-CONSENSUAL PORNOGRAPHY)

Cyber pornography is defined as transmission, storing, and receiving sexually explicit images /pictures of women in cyberspace. Cyber pornography is alarming which is evident from the following statistics. According to Sinha and Pendyala, the number of pornographic websites is 4.2 million, which is 12% of total websites. The daily pornographic search engine requests are 68 million (25% of search engine requests). 42.7% of Internet users view pornography. According to National Crime Records Bureau data, the number of cases for obscene publication and transmission in electronic form under the Information Technology Act, 2000, has been reported in the increasing trend since 2007, when 99 such cases were reported. The number rose to 105 in 2008, 139 in 2009, 328 in 2010, 496 in 2011, and 589 in 2012. The figure more than doubled to 1,203 in 2013. In 2014, 758 crimes were reported, of which 491 people were arrested.

An NGO in India, Cyber & Law Foundation, conducted a survey in 2016, where it was revealed that as many as 27% of internet users, mostly between the ages group 13-45, have been subjected to revenge porn**.** According to the NCRB (2014), in India, the total number of cases registered in the year 2014under cybercrimes was 7,201. Of which, 758 (10.5%) cases were related to publication/transmission of obscene and sexually explicit content and 491 persons have been arrested in connection with cyber pornography[10]. The Pew Research Center's Internet and American Life Project (2010) conducted a study, examining data on sending and

[10] Aritra Sarkhel, 'The wrath of Revenge porn in India' (*The Economic Times: Tech,* 13 November 2017) <https://tech.economictimes.indiatimes.com/news/internet/the-wrath-of-revenge-porn-in-india/61633860> accessed 03 February 2022

receiving of sexually nude or semi-nude images by American adolescents and adults. The study found that adults who belonged to the age group of 18 years and above had sent sexually suggestive images (6%) and 15% had received such texts. The prevalence of sending and receiving sexually suggestive nude or nearly nude photos differed between age groups[11]. According to a survey conducted in 2016 by Cyber & Law Foundation, an NGO in India points out that 27% of internet users aged 13 to 45 have been subjected to revenge porn or other cybercrime-related cases. Due to the fear of the stigma attached to this and the lack of any concrete law which deals with revenge porn, victims often end up not reporting these crimes[12].

MORPHING

In morphing, the original pictures of people were downloaded by the offenders and were altered with pornographic images with malicious intention to defame them. Deep Nude, the website basically used for morphing requires a user to upload any picture and within seconds generates a nude version of the subject of the picture, which is typical of women (basically morphed pictures of females). Experts said that once a nude of any woman was generated, the possibilities for misuse were endless. Civilian cyber expert Shubham Singh said, "We have received information about pictures of women being morphed using Deep Nude and being used for nefarious purposes like blackmail, pornography and creating catfish accounts on dating apps"[13].

REVIEW OF LITERATURE

As per NCRB data, there was a 104 percent increase in the volume of obscene content shared electronically between 2012 and 2014 alone. A 2010 cybercrime report uncovered that only 35 percent of females reported the incident. It also states that 18.3 percent of females were not even aware of their victimization in cyberspace. Another recent research conducted by

---

[11] Amanda Lenhart, 'Teens and Sexting' (*Pew Research Center,* 15 December 2009) <https://www.pewresearch.org/internet/2009/12/15/teens-and-sexting/> accessed 03 February 2022

[12] 'Awareness: Revenge Porn Victim Actress Speaks About How It Changed Her Life' (*The Indian Feed,* 27 November 2017) <https://www.theindianfeed.in/revenge-porn-awareness/> accessed 03 February 2022

[13] Gautam S. Mengle, 'Law enforcers worried as Deep Nude makes a return' (*The Hindu,* 13 May 2020) <https://www.thehindu.com/news/national/law-enforcers-worried-as-deep-nude-makes-a-return/article31334415.ece> accessed 03 February 2022

Feminism in India (FII) and part of Freedom House Hyper-linkers on 'Violence online in India: Cybercrimes against women and minorities on social media,' found that 50 percent of women in urban areas experienced online abuse.[14] Cybercrimes pose a great threat to individuals, especially women, who form 90 percent of the victims. Every second, one woman in India gets tricked to be a victim of cyber crimes and the online platform is now the new platform where a woman's dignity, privacy, and security are increasingly being challenged every moment. **Halder and Jaishankar (2010)** have found in their study that more than half of the female respondents of the total 73 respondents were victims of cybercrime. The respondents stated about 29 forms of cybercrime victimization which includes abusive, obscene, and dirty messages (85%), repeated emails asking to befriend them (16.7%), threat emails and messages from ex-partners and husbands (50%) followed by sexually teasing remarks in their social networking profiles and email (75%), hacking (48.3%), stalking (40%), phishing attack (43.8%), impersonation (61.7%), cloned profiles (50%), cyber defamation (71.7%), hate messages (41.7%), bullied (33.3%) and morphing (33.3%). Also, 45.5% were targeted for their lifestyle choices, sexuality, and feminine ideologies.

RESEARCH METHODOLOGY AND BRIEF OUTLAY OF THE PAPER

The present paper precisely focuses on the cyber victimization of females studying in higher education institutions in India. This study uses the Exploratory Research design to demonstrate the phenomenon of Cyber Victimisation of female students in our country. The collection of the relevant data is in online mode due to restrictions relating to the coronavirus pandemic. This method also provides a better outreach to victims from different institutions having female students. Data were from both primary and secondary sources. The Primary data included responses from a sample of 200 respondents' female students enrolled in higher education institutions of India using a non-probability sampling technique with a convenient sampling method. The secondary sources include literature reviews, articles, journals related to cybercrime against females. A questionnaire including both open-ended and close-ended

[14] Shreya Kalra 'Survey Finds Nearly 50% of Women In Indian Cities Face Online Abuse, Fewer Report Them' (*India Times,* 6 December 2016) <https://www.indiatimes.com/news/world/survey-finds-nearly-50-of-women-in-indian-cities-face-online-abuse-fewer-report-them-266051.html> accessed 03 February 2022

questions in a structured form was tailor-made for this study. Overall, this study used mixed research methods using both qualitative& quantitative modes of inquiry. Thus, the present paper provides details of the findings of this study conducted in the year 2020 with 200 female respondents across India.

THE RATIONALE OF THE STUDY

Digitalization has led to an increase in the number of internet users sharply across the world. However, those people especially females, who are lacking in education and awareness about cyberlaw, cybercrime, and technology, can easily be targeted by predators. These days cybercrime against females is on the rise and most of the crimes go unreported to law enforcement agencies due to lack of support or pressure on the victim, especially in the case of the known perpetrator. The study is relevant as it emphasizes the fact, that the problem of cybercrime against females can be controlled and thereby prevented by educating them about technological measures and an effective Cyberlaw (IT Act) which includes well-defined legal provisions related to Cybercrime against females. The study aims to gain familiarity about the trend of Cyber victimization among female students of higher education institutions, the relationship between victim and perpetrator if it exists, and the frequency of reporting to the law enforcement agency.

STATEMENT OF THE PROBLEM

Cybercrime is a growing menace which increased in recent times that requires the immediate attention of Law enforcement Agencies, Cyber Officials, government, and common-men. Limited authenticated and reliable statistics are available on the nature of Cybercrime against females because most of the cases are unreported due to the fear of labeling by society and victim-blaming. This field requires a more effective study due to the increase in the number of Cybercrime against females and internet users. So hereby this study attempts to find the prevalence and reasons for the victimisation of female students on the Internet, relation with the perpetrator, and dark figures in it in India.

OBJECTIVES OF THE PRESENT STUDY

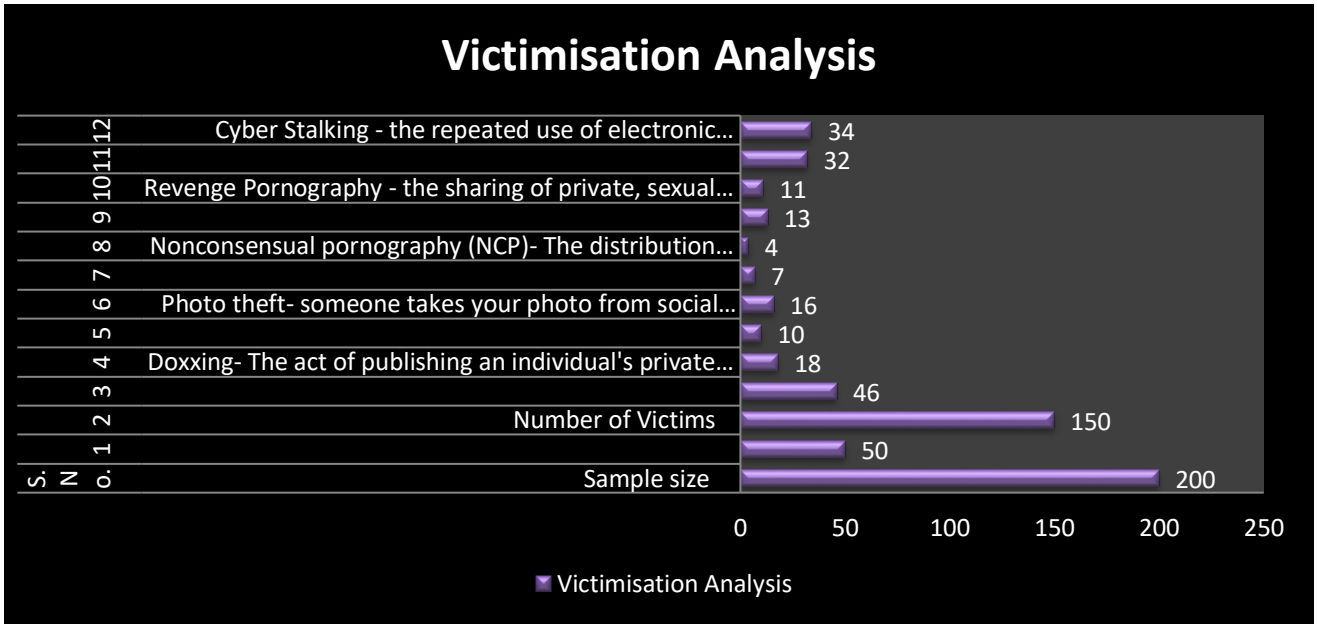
The present paper investigates the prevalence of Cybercrime against female students and the dark figures (if any) in India. It also tells about the reasons for the Victimisation of females in Cyberspace from the victims' perspective. It gathers knowledge about the present scenario regarding specifically reporting Cybercrime against female students in India. This paper analyses and presents information about the Victim and Perpetrator in terms of known/unknown in the event of Cybercrime. Lastly, the paper also provides suggestions regarding measures for dealing with the problem of Victimisation of females in Cyberspace in an effective way.

LIMITATIONS OF THE STUDY IN THE PRESENT PAPER

This study is limited to female students of higher education institutions. Also, it is not considering financial cybercrime since it is out of the purview of the problem under investigation. The paucity of time and paucity of resources were reasons why large samples could not be drawn for a longer period of time.

DATA ANALYSIS

Graph 1.1 About Victimisation Analysis



This graph shows the number of females victimized in Cyberspace. Most of the respondents were the victim of Cyberstalking (34) followed by Cyber harassment (32) and Non-consensual Pornography having the least number (4) of the total respondents as per the survey report.

Table 1: About mode, time and reason of internet usage

**N denotes the number of respondents & % denotes the percentage

Table 1: About mode, time and reason of internet usage

**N denotes the number of respondents & % denotes the percentage

1.	Medium of internet access	N	%
	Personal Smartphone	188	93.5
	Shared/Parent's/ Sibling's phone	6	3
	Personal laptop/ tablet	7	3.5
2.	Time spend online daily		
	1 hour	15	7.5
	2 hour	37	18.4
	3 hour	49	24.4

	4 hour	41	20.4
	more than 5 hour	52	25.9
3.	Reason for spending time online		
	Due to loneliness	66	32.8
	Due to lack of emotional support	9	4.5
	Due to stress	20	10

This table states that (93.5 percent) of respondents use their smartphones for accessing the internet and the maximum number of respondents (25.9 percent) use the internet for more than 5 hours and 32.8 percent. Respondents in the majority state that they are using the internet due to loneliness.

Table 2: About cyber harassment

Cyber harassment	N	%
Approached for sexual favors on the Internet		
Not a victim	102	50.7
Yes	31	15.4

No	68	33.8
Subjected to sexual colored remarks		
Not a victim	96	47.8
Yes	34	16.9
No	71	35.3
Shown pornographic content without consent		
Not a victim	93	46.3
Yes	17	8.5
No	91	45.3
demanded unwelcome physical, verbal or non-verbal conduct of sexual nature		
Not a victim	93	46.3
Yes	27	13.4
No	81	40.3

This table shows that 16.9 percent of respondents were victims of Cyber harassment. 15.4 percent were approached for sexual favors, 16.9 percent were subjected to sexually coloured remarks, 8.5 percent of respondents' pornographic content shown without consent on the internet and 13.4 percent were the victims of demanding unwelcome physical, verbal or non-verbal conduct of sexual nature.

Table 3: About victimization through cyberstalking

Cyber Stalking	N	%
Anyone following your activities		
Not a victim	91	45.3
Yes	32	15.9
No	78	38.8
If yes then how		
Not a victim	91	45.3
By posting messages	16	8
By entering into a chatroom	7	3.5
By constant emails	4	2

Others	82	41

This table shows that out of the total sample 15.9 percent of respondents were victims of cyberstalking and 8 percent of respondents were victimized by posting constant messages on social media on the internet.

Table 4: About victimization through revenge pornography on the internet

Revenge Pornography	N	%
Anyone ever shared your private/intimate photos or videos without consent to take revenge		
Not a victim	111	55.2
Yes	11	5.5
No	79	39.3
If yes then related to the perpetrator		
Not a Victim	187	93.5
Relative	1	0.5
Acquaintance	1	0.5

Friend	6	3.1
Unknown	5	2.6

This table shows that 5.5 percent of respondents were the victim of Revenge Pornography and 3.1 percent of the perpetrator was a friend.

Table 5: About victimization through doxxing

Doxxing	N	%
Posted email addresses on public websites with the intention to harm		
Not a Victim	125	62.2
Yes	8	4
No	68	33.3
Shared contact details without consent		
Not a Victim	121	60.2
Yes	18	9
No	62	30.8

Posted home addresses on public websites without knowledge/Consent		
Not a Victim	128	63.7
Yes	4	2
No	69	34.3

This table shows that 9 percent of respondents were victims of Doxxing out of which the email address of 4 percent of respondents was posted on the internet, the home address of 2 percent of respondents were posted on public websites, and contact details of 9% of respondents were shared on the public website without consent by the perpetrator.

Table 6: About victimisation through morphing and photo theft

Morphing & Photo theft	N	%
Edited original picture and shared without consent		
Not a victim	123	61.2
Yes	13	6.5
No	65	32.3
Took a photo from social media and posted it to harm the image		

Not a victim	121	60.2
Yes	16	8
No	64	31.8

This table shows that 6.5 percent of respondents were the victim of morphing where the perpetrator edited the original picture of a respondent and shared it anywhere across the internet.8% of respondents state that they were the victim of photo theft where the perpetrator took the photo from social media and posted it to harm the image of respondent across the internet.

Table 7: About victim-perpetrator relationship

Victim Perpetrator relationship	N	%
Perpetrator was known		
Not a Victim	50	25
Yes	19	9.5
No	121	60.5
Can't say	10	5
Relation if known		

Not a victim	50	25
Boyfriend	2	1
Friend	10	5
Acquaintance	5	2.5
Not known before the incidence	130	65
Reason behind victimisation		
Not a victim	50	25
For fun	20	10
For revenge	5	2.5
To harm image	9	4.5
Don't know	116	58
Age during victimisation(in years)		
Not a victim	50	25
Below 18	9	4.5

18-21	30	15
21-24	101	50.5
Minor during victimisation		
Not a victim	50	25
Yes	12	6
No	138	69
If minor then age group(in years)		
Not a victim	50	25
Below 14	1	0.5
14-16	8	4
16-18	3	1.5
Not a minor	138	69

This table shows that 9.5 percent of respondent states that the perpetrator was known, 5 percent states that the perpetrator was a friend and 65 percent states that the perpetrator was not known before the incidence and 10 percent of respondent states that the reason behind the

Victimisation was fun and 50.5 percent respondents were victimized during 21-24 years and 6 percent respondents were minor during victimization.

Table 8: About reporting of cybercrime

Reporting	N	%
Reported the incident		
Not a victim	50	25
Yes	12	6
No	138	69
Support from LEA		
Not a victim	50	25
Yes	4	2
No	7	3.5
Not reported	143	71.5
Aware about cyber security helpline		
Yes	151	75.5

No	49	24.5
Females are safe on the internet		
Yes	37	20
No	72	39.1
Maybe	65	35.3

This table shows that 6 percent of respondents reported the incident and 3.5 percent of respondents didn't get better support from LEA and 75.5 percent of college-going females are aware of cyber security helpline and only 20 percent of females think that they are safe on the internet.

FINDINGS

The age group of respondents & about the device: In this study, fifty percent of the respondents belonged to the age group of 21-23yrs. Out of which, a majority of the respondents i.e. 93.5 percent reported using their personal smart-phone to access the internet followed by 3 percent using a shared/ parent's smart-phone. 3.5 percent of the respondents mentioned that they use their personal laptop/tablet.

Duration of cyber access and corresponding reasons: One-fourth of the total respondents i.e. 25.5 percent spend more than five hours daily on the internet. The data indicates that 32.8 percent of the respondents spend more time online on daily basis due to loneliness followed by (10) percent of the total respondents due to stress.

Literacy status of respondents: Regarding education status, 46.8 percent of the total respondents were pursuing graduation at the time of data collection i.e. the year 2020.

Prevalence of cyber victimisation of females: Out of the total respondents in the present study 75 percent of them informed that they were victims of Cybercrime.

Nature of cybercrime: The data implies that 15.4 percent of total respondents were approached for sexual favors on the internet. Nearly 16.9 percent of respondents were subjected to sexually coloured remarks on the internet. Data also reveals that pornographic content was shown without consent to 8.5 percent of total respondents in this study. Almost 13.4 percent of the respondents were demanded unwanted physical, verbal, or non-verbal conduct of sexual nature. 15.9 percent of the respondents were victims of stalking. Nearly 8 percent of the respondents reported that they were harassed online by posting messages. Data shows that 5.5 percent of respondents were victims of Revenge Pornography.

Nature of relationship with offender in terms of known/unknown etc.: In this study, 3.1 percent of the respondents state that the perpetrator was related/ known to them as a friend. Responses indicated that the perpetrator was known to nearly 9.5 percent of respondents. It is also inferred that 5 percent perpetrator was a friend.

More on Cybercrime: Nearly 02 percent of respondents were the victim of Non-consensual pornography out of which 01 percent of respondents shared the images or videos by their own consent but later the same was misused by the perpetrator. It is found that 9 percent of respondents were the victim of Doxxing. Data indicates that 6.5 percent of respondents' original photos were edited and shared on the internet to harm their image. Nearly 8 percent of respondents state that their photos were taken from social media and posted anywhere on the internet with the intention to harm the image.

Regarding reasons for victimisation: Nearly 10 percent of the respondents state that the reason behind their victimization was fun, followed by 4.5 percent to harm the image and 2.5 percent for revenge.

Characteristics of Victims of cybercrime: It was found that 4.5 percent of respondents were minor during their victimization. Nearly half of the victims i.e. 50.5 percent belong to the age group of 21- 24 years and 04 percent of minor victims belong to the age group of 14-16 years.

Reporting the cybercrime incident to Authorities: Nearly 06 percent of the total respondents reported the incidence of Cybercrime to authorities. **More than half of the respondents 69 percent have not reported the incident of Cybercrime**.

More on reporting the cybercrime incident to Authorities: Only 02 percent of respondents get better support from law enforcement agencies after reporting the incident. It was found that a total of 24.4 percent of respondents are not aware of Cyber Security Helpline.

Perceived safety in Cyberspace/fear of cybercrime in cyberspace: Almost 20.1 percent of the total respondents think that females are safe on the internet.

DISCUSSIONS

After analyzing the responses of participants, the finding of the present study in this paper suggests the following factors as the reason for victimisation:

Psychological reasons include stress, loneliness, and lack of emotional support:

Stress: As we are moving to the digital era then this cyberspace become a most important part of life and females try to connect with friends through social networking sites but during stress, they can easily fall prey to perpetrators as found out by researchers after analyzing the responses of participants.

Loneliness: Loneliness is the major reason for victimization because at that time the female tries to make friends on social networking sites where the friend she made can be a perpetrator the study reveals 5% of perpetrators are friends.

Lack of emotional support: in this, the female seeks emotional support from virtual space friends and after gaining the trust of the female the perpetrator can easily victimize them.

CONCEPTUAL MODEL ON REASONS OF VICTIMIZATION

This study develops two models on the reasons for victimisation and the motives of the perpetrator behind Cybercrime.

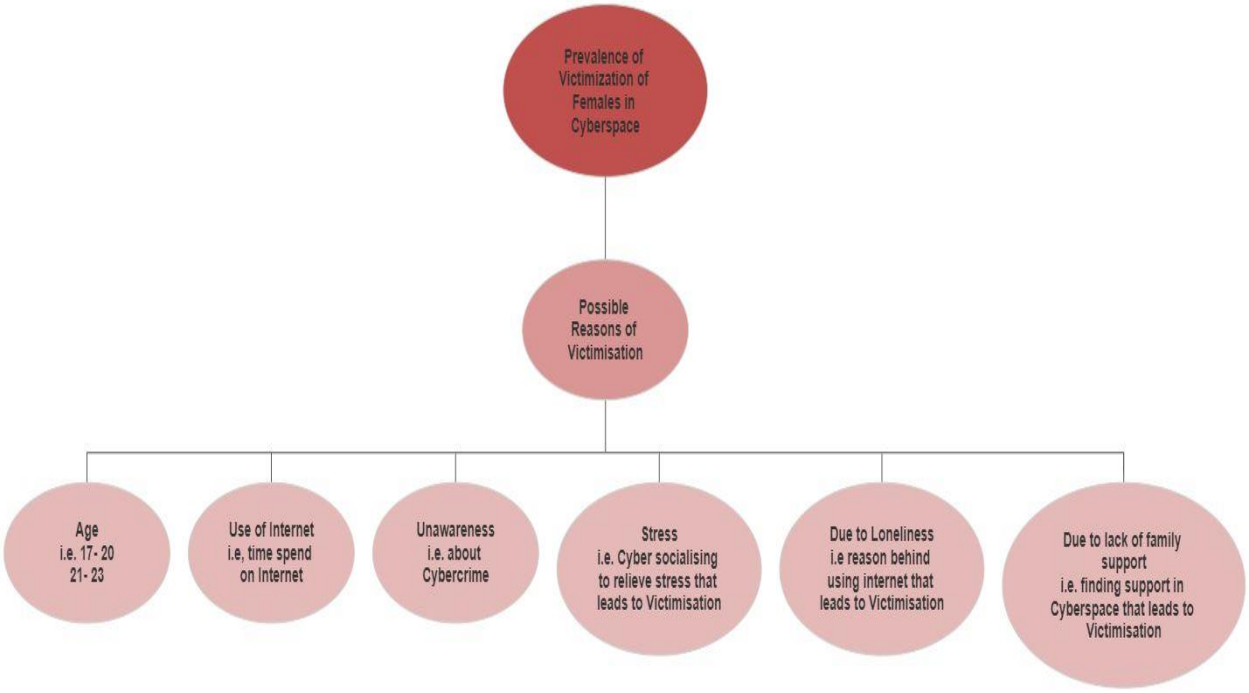
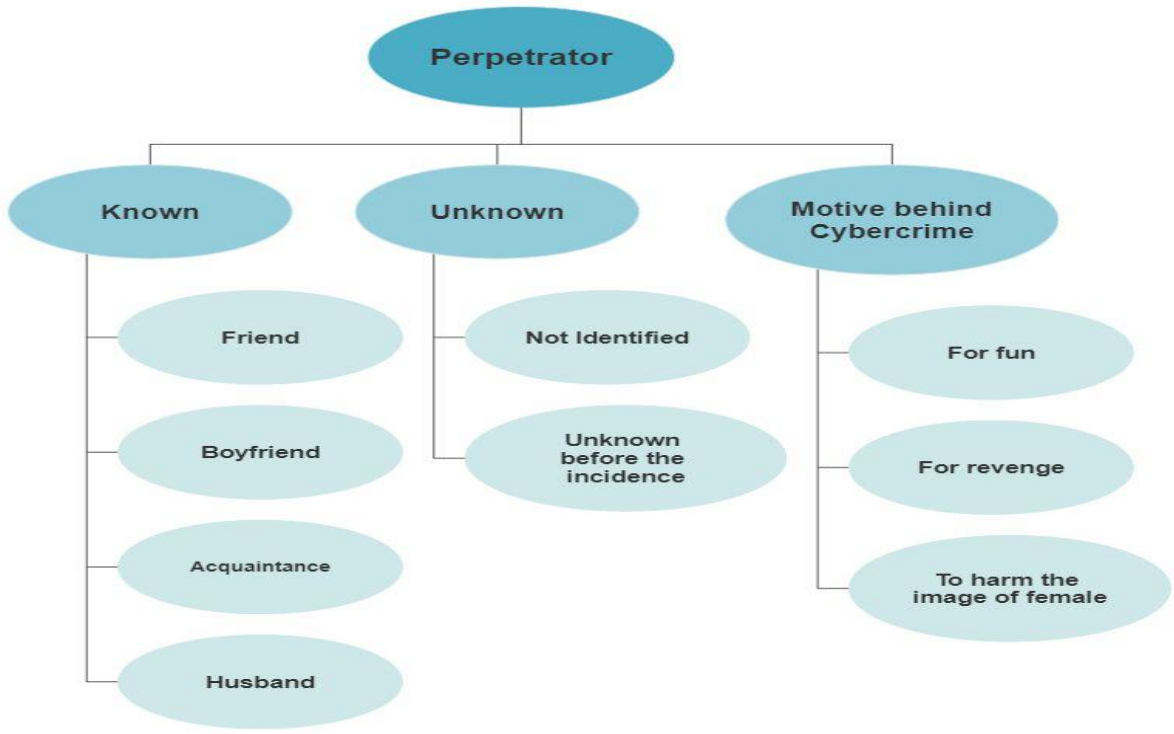


Figure1.3. A conceptual model to identify the perpetrator and its motive behind cybercrime



The findings of the present research study indicate that most of the perpetrators were unknown before the incidence and in the case of the known ones; most of the perpetrators

were a **friend.** The motive behind the cybercrime in most of the cases was fun followed by revenge and in some cases harming the image of females. This resulted in the researcher representation of the concluded model on perpetrator and motive behind cybercrime from the victims' perspective.

SUGGESTIONS

General Suggestions

Avoid friendship with strangers on social networking sites as it may reduce the chances of unnecessary victimisation in cyberspace. One should always be updated about knowledge regarding cyberspace, cybercrime, and cyber law. Individuals should block and report all the accounts which bully or harass and inform the same as soon as possible to the authorized person i.e. Parents & Police to avoid more harm. Avoid sharing passwords and personal information because that person can misuse the information or may have unauthorized access to your account in your absence. Individuals should opt for two-step verification on apps wherever it is possible. It helps in enhancing the security of the app so that perpetrators can't easily have access to the account. Individuals should be careful while using a webcam because the perpetrator can have access to the camera through hacking or by means of malicious links so it is suggested to cover the laptop/ Smartphone camera with tape or paper while not in use. Individuals should avoid free downloading sites as their files may contain viruses or Trojans. Individuals should avoid unnecessary posting and sharing of pictures in any group where the members are not known or on any public websites. Individuals should be carefully aware of terms and agreements while using dating apps. Individuals should avoid clicking on suspicious links this can be a phishing attack by a perpetrator to have access to your device. Individuals should ensure that their social media accounts are private. It reduces the chances of victimization by the unknown, as by this setting only enlisted friends have access to the pictures and other information. Individuals should use a variety of passwords for all social media accounts and change the passwords from time to time and also ensure that it is strong.

Individuals should use spamming filters/ spyware detectors and cleaners regularly to avoid malicious emails, trojans, viruses, etc...

Individuals should read carefully the terms and conditions before clicking on agreeing to maintain privacy. Individuals should avoid installing apps from unauthorized sources because they may contain a virus, Trojans, etc... Through this, the perpetrator can have access to the phone. Individuals should note that www.cybercrime.gov.in is the reporting portal where everyone including females can report anonymously without disclosing their personal details.

Suggestions for parents/ guardians

- Parents/ Guardians should make their child aware of the pros and cons of the internet so that he/she can safely surf the internet.
- Parents/ Guardians should make their children social in the physical world instead of cyberspace so that they will not become netizens at an early stage.
- Parents/ Guardians should be friendly with their children and don't blame them for their actions so that they can share any incident without any fear.
- Parents/ Guardians should block adult websites in their children's smartphones/laptops if they are minors.
- Parents/ Guardians should keep a watch on their child's online activity if he/she is a minor.

Suggestions for Law officials:

- There should be well-defined cyber laws for cybercrime against women as the cases are increasing day by day so it's a need of the hour.
- The punishment should be stringent for these cybercrimes to create a deterrent effect on perpetrators.
- Awareness programs should be conducted for students

Suggestions for technical professionals:

- There should be an age restriction or age verification steps on adult websites for preventing access to minors.
- Social media should be able to recognize which are legal profiles and which are fake profiles through valid identity verification to avoid fake profiles on social media.
- Applications should be launched with extra security features.

Suggestions for Law Enforcement Agencies

- Cyber police personnel should be trained in sensitively dealing with victims of cybercrime as it can increase the rate of reporting.
- Immediate response should be taken by Law enforcement officials so that the victim can be well redressed.
- More Cyber cells in police and exclusive Cyber courts are the need of the hour by seeing the rapid increase in cybercrime cases.
- There should be female officers to deal with female victims so that females can share their traumatic experiences easily.
- There should be a cyber forensic expert for an investigation to deal effectively with pieces of evidence of cybercrimes.

Suggestions for teachers and Professors:

- Awareness of cybercrime and cyber laws should be a regular course in educational institutions.
- Proper guidance and education should be given at schools and colleges through a seminar to students to make them aware of the usage of cyberspace and issues related to it.