DIGITAL VICTIMIZATION OF WOMEN IN CYBERSPACE: AN ANALYSIS OF EFFECTIVENESS OF INDIAN CYBER LAWS

Ms. Akanksha Pathak[1]

Mr. Prateek Tripathi[2]

ABSTRACT

A considerable part of cyberspace is full of unexpected outcomes. This is the result of misfeasance, malfeasance as well as nonfeasance. The target group of such activities are the vulnerable sections of the society which includes women, children and senior citizens. Cybercrime has an intrinsic changing pattern, which targets distinctive groups differently. Women are more prone to being digital victims of sexual offences. Technology like deep fake morphing can be used in various sexually explicit materials to victimize women for different cybercrimes. Such crimes have affected women of every strata of society. According to a government report, around 11,000 cases have been registered in 2021 which categorically falls under cybercrimes against women. This figure was around 6,000 in 2018. However, the increment in reported cases does not necessarily result in conviction. The intricacies of proving such offences becomes a daunting task for professionals. The ramification of such inefficiency results in a breakdown of women victims to fight their cases. This leads to psychological, physical as well as societal degradation of women's position. The government has introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to make cyberspace safer for each group. In addition, the Ministry of Home Affairs operates a National Cyber Crime Reporting Portal to enable citizens to report complaints pertaining to all types of cybercrimes, with a special focus on cybercrimes against women. Such positive steps would require close scrutiny to secure cyberspace and to reduce the digital victimization of women. This paper analyses the cybercrimes and their effect on women by highlighting the causes. Moreover, the other

[1] Research Scholar at Dr. Ram Manohar Lohiya National University, Lucknow.
[2] Senior Research Fellow at Faculty of Law, University of Lucknow.

part of the paper delves into the legal discourse and the effectiveness of contemporary solutions.

Keywords: *Digital Victimization, Cybercrime, Information and Technology Act, 2000, Sexual Harassment, Cyber Space.*

INTRODUCTION

The internet is one of the greatest sources of information and support one can have in the present era of modernization and technological advancement. The internet has made the world a global village and it's bound to do more in future. It has given so many avenues of growth to human beings from online businesses, jobs, websites, advocacy, political campaigning and even socialization. The internet and its community have offered many places for people to engage with their thoughts without any hesitation. It has led to many types of activism and debates. It has led to people coming out of their boxes and engaging in meaningful conversation. Social networking sites such as Twitter, Facebook, Instagram and other dating apps at present have given netizens a wide variety of activities to engage in. These social networking sites have provided a participatory and all-inclusive, open public environment with which many can have all-around inclusive development.

But the internet and these social networking sites have a dark side too. Online platforms often tend to be hostile places where people's voices are shunned if they speak anything against the crowd. Many are shut down from further participation with online abuses and different types of cybercrimes.

Our social structures and legal environment have failed to handle the situation and lack the technological advancement to catch the perpetrators of crime which often leads to victimization of the person who has been abused. The anonymity of data is one of the important tools applied by many developed countries to hide the identity of the person and secure their data even at the time of data leaks, but the same anonymity

becomes evil when it is used by the perpetrators of crime to hide their identity online once the crime has taken place.[3]

Digital Victimization is not a new phenomenon - wherever there have been cybercrimes, victimization has existed but for a long time. We have only been concerned with defining and understanding crimes and their types and what technology to employ to catch the perpetrators and not focused on digital victimization and its causes and how that can be tackled.

Digital Victimization has taken men and women both into its hands but women often tend to be more vulnerable than men. Recent studies have shown an alarming increase in the number of women who have faced online abuses such as bullying, morphing images, deep fakes, stalking, voyeurism etc. Often social media and its open access provide a great opportunity for such crimes with abuses focusing towards sex/gender stereotyping.

Many incidents have taken place in the world including India which have led to digital victimization and often technological advancement of perpetrators of crime developing at much faster speed than any legal framework of a nation which provides benefits to them.

TYPES OF CYBERCRIME LEADING TO DIGITAL VICTIMIZATION

Cyberbullying, cyberstalking, cyber hacking and phishing are the most common types of cybercrimes happening all over the world. With new social networking sites and public profiles, perpetrators or hackers can't get happier. There are other types of crime that have developed due to these social networking websites like trolling, making fake profiles, morphing images, cyber abuse, defamation and others.

[3] Kim Barker and Olga Jurasz, 'Online Misogyny' [2019] JoIA, 95, 114.

Let us first understand these crimes and their meaning.

Cyberbullying has been defined as bullying a person on different mediums such as social media, dating platforms, and gaming using digital technologies which aims at threatening or shaming any person who is being targeted. Examples of it can be sending and spreading wrong messages and images about a person which tends to lower his reputation and makes him a laughing stock.[4] Cyberbullying is often a gender neutral offence which can take place against men and women both and teenage children are the most targeted groups. A targeted person is often harassed about his looks, body, family, race, religion, dressing sense, attitude, financial condition etc.[5]

Stalking simply means to look or search for a specific person. It can be done physically also and when it is done online it becomes cyberstalking and when a person is harassed while stalking or some fear of harm is asserted as the result of such stalking it becomes a crime. In some jurisdictions, cyberstalking is committed when some overt act or conduct takes place against the victim otherwise it's not considered as a crime and in some jurisdictions, mere fear in the mind of the victim due to stalking is a substantive crime.[6]

Cyber Harassment means sending threatening messages or emails or creating impersonating profiles and websites targeted at harassing a particular individual.[7] In many jurisdictions and in India, cyber harassment also includes sexual harassment of

---

[4] 'Cyberbullying: What is it and how to stop it' <https://www.unicef.org/end-violence/how-to-stop-cyberbullying> accessed 14 March 2023.

[5] Andrew M. Henderson, 'High-tech words do hurt: A Modern Makeover Expands Missouri's Harassment Law to Include Electronic Communications' [2009] 74 MoLR 379, 3; See also K. Jaishankar, 'Cyber Bullying in India: A Research Report on developing Profile' [2008] Legal Reviews and Policy Guidelines. Tirunelveli, India.

[6] Naomi Harlin Goodno, 'Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws' [2007] 72 MoLR 125, 126.

[7]Telecommunications & Information Technology, 'State Cyberstalking and Cyber harassment Laws', (*NCSL* 16 November 2012) <http://www.ncsl.org/issues-research/telecom/cyberstalking-and-cyberharassment-law s.aspx> accessed 15 March 2023.

victims which includes physical contact and advances, making sexual remarks and asking for sexual favours.[8]

Social Media or Digital Impersonation means creating a fake profile, email ID or website of a person without his or her consent with the intention to harm the reputation of a person. Perpetrators often make a 'fake avatar'[9] of the individual and we see this in our everyday life as fanmade pages of celebrities often with their names. But the problem arises when these fake profile pages are used to blackmail by making untrue statements about them or asking for financial gains from the followers or connections of those accounts in the name of such persons.[10] In 2020, Karnataka recorded the highest number of digital impersonation cases than the rest of the country. In total, India recorded 11 thousand cases in which 6 thousand alone were recorded in Karnataka.[11]

Cyberbullying and cyber harassment are not very similar to cyberstalking as one is concerned with communicating fear by words written or spoken on any platform while stalking requires credible threat or some commission of such threat to arrest the predators.[12]

Trolling means when a person tries to deliberately stir up any disagreement, animosity, or argument in an online social network. Trolls may target websites like YouTube's comment sections, forums, or chat rooms.[13]

---

[8] The Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act 2013, s 2(n).

[9] Debarati Halder, 'Examining the Scope of Indecent Representation of Women (Prevention) Act, 1986 in the Light of Cyber Victimization of Women in India' [2013] 11 NLSJ 188.

[10] Trends and Transitions, 'Internet Imposters' (*NCSL*, May 2010) <http://www.ncsl.org/magazine/trends-and-transitions-may-2010> accessed 15 March 2023.

[11] Tanushree Basuroy, 'Number of online impersonation offenses reported all over India' (*Satista* 14 Oct 2022)<https://www.statista.com/statistics/1097572/india-number-of-online-impersonation-offences-by-leading-state/> accessed 15 March 2023.

[12] Cassie Cox, 'Protecting Victims of Cyber stalking, Cyber Harassment, and Online Impersonation through Prosecutions and Effective Laws' [2014] 54 Jurimetrics 277.

[13] The Now, 'What is trolling?' (*GCF Global)* <https://edu.gcfglobal.org/en/thenow/what-is-trolling/1/> accessed 15 March 2023.

Trolls frequently utilize emotionally charged statements to elicit replies from individuals, disturbing normal civil discourse. Anywhere there is an open forum where people are free to publish their ideas and opinions, trolling can happen.[14] Trollers use their advantage of freedom of speech and expression to disrupt normal communication with their own set of offensive comments. Trollers nowadays have started using pictures, movie images, songs, taglines of ads, movies and songs to create a different meaning of the same image and it has become so popular that even many businesses are using it to grab the attention of the public instantly and even few government agencies have also started using it. Many times these trolls get so offensive that they tend to hurt the sentiments of public or religious groups. Trolling and cyberbullying often can be turned into mob lynching either virtually or physically through various forums like Whatsapp and Facebook where a large group can bully another person or group for their religious, racial, political and national beliefs.

Phishing is the most common of cyber-crimes at present time and anyone even the most educated can be easily lured into this. Phishing is a fraudulent act of obtaining personal information such as ATM password, OTP, bank account details, debit card details and personal account password over mail, telephonic communication and online websites.[15]

Firstly, the hackers create a deceptively similar website of the desired institution like your bank or an online shopping site then when you open such a site and enter your details on the pretext of considering it the original website the hackers save the data and password entered and use it further to your disadvantage.[16] This type of crime often depends on the knowledge and awareness of the victim and not only the illiterate persons are a bait to such crimes but also the most educated youngsters as well as retired senior citizens. India has seen a steep rise in such number of crimes especially in bank frauds which has led all banks to issue advisories to its citizens and customers. All

---

[14] 'Jade Goody Website troll from Manchester jailed' (*BBC* 29 October 2010)<http://www.bbc.co.uk/news/uk-england-manchester-11650593> accessed 15 March 2023.
[15] Alice Hutchings & Henessey Hayes, 'Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the Net' [2009] 20 CRIM.Just 433.
[16] Ibid.

banks suffered a loss of 160 crore in the 2020 financial year and 128 crore in the financial year of 2021.[17] According to Lynch "phishing" comes from the word fishing as email, telephonic conversations and online websites are used as a bait to attract "fish" from the "sea" of online users of internet.[18]

Morphing means to change something or someone from one thing to another.[19] Morphing images has the same meaning. When an image is said to be morphed, it signifies one has tampered with the original image without that person's consent. The case of actor Ranveer Singh's images which he complained had been morphed is an example of how easily it can be done.[20] In the world of influencers and bloggers, one can easily get a picture of anyone and if they have a public profile, it all becomes so easy. Morphing an image has also been so easy with specific apps coming for the needful job. All over the world, women become easy prey to it as they are more vulnerable due to easy character assassination and stigmatization. If such an image is circulated over the internet in minutes, the reputation of such persons is shattered in seconds and such person is often seen disgracefully by society itself which leaves a permanent scar of victimization on the persons. Perpetrators often ask for money and other valuable property on the promise of not circulating such images on the internet which leads to harassment of the women. India has alone recorded 37% of cases related to harassment of women due to morphed images.[21] Images are morphed with sexual content generally which is also known as deep fake technology. This leaves a tragic fear in the mind of the person whose image is morphed and such person is victimized for many years.

These are a few, most popular cyber-crimes happening in the present world. As we know, year by year, the world is growing and innovations are taking place in all the

---

[17] 'Govt shares data on online banking fraud and how many cases solved' (*livemint,* 9 August 2022*)* <https://www.livemint.com/news/india/govt-shares-data-on-online-banking-fraud-and-how-many-cases-solved-11660007363092.html> accessed 15 March 2023.

[18] J Lynch, 'Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks' [2005] 20 Berkeley Technology Law Journal 259.

[19] 'Morphing' <https://dictionary.cambridge.org/dictionary/english/morphing> accessed 15 March 2023.

[20] 'Photo Morphing Cases', (*Times of India)* <https://timesofindia.indiatimes.com/topic/photo-morphing-case/news> accessed 16 March 2023.

[21] '37% of harassment cases is by morphing photos of women', (*The Hindu,* 28 July 2021)<https://www.thehindu.com/news/cities/Hyderabad/37-of-harassment-cases-is-by-morphing-photos-of-women/article35591294.ece> accessed 16 March 2023.

fields. Thus, technology grows at much faster speed than our laws which could supplement such technological advancement. Laws of a country are formed over deep discussion and research and it's not so easy to change and alter law every other year which allow these predators to take advantage of lacunas in law and commit crimes. However, this is not the sole reason which offers bait to these perpetrators. There are further reasons why these crimes are happening and how one chooses his fish in the sea of online users. In the next section of this article, we will study different causes leading to digital victimization.

DIGITAL VICTIMIZATION: CAUSES AND FACTORS

There can be many causes of victimization like digital illiteracy, psychological, social and legislative gaps. The advent of the internet has benefited human civilization. The internet has united people together globally. Human nature demands that we always want to know more about the unknown. The drive to find the untrodden road has been exacerbated by a curiosity about the inhabitants of the planet. This has caused the digital universe to be discovered.

Theory of Routine Activity

According to routine activity theory,[22] crime generally occurs when one is busy in their routine lives and a target is set whenever such a suitable person comes in front of an offender who is motivated to commit such a crime. Lack of a guardian, less knowledge of computers and internet experience and high banking transactions can give an offender an easy target for attacking such person's bank account through phishing attacks. Such attackers hide their identity through various anonymity technologies and commit crimes by sitting anywhere in the world. An attacker may sit in any corner of the world and commit an attack in India and vice-versa. Such international phishing attacks often give offenders the leverage to not get punished due to lack of legislative laws regarding such cross-border attacks. Often when the crime is reported money is given

[22] Hutchings (n 15).

back by the financial institutions but the offender is not punished which acts as motivation to such offenders.[23] Most of the phishing sites are hosted by the US, China and Russia because there exist a high number of internet users compared to least developed countries. India and Thailand also come under the top ten countries hosting such sites.[24] Absence of a guardian means lack of proper guidance and expertise and awareness of these financial institutions, banks, legislative departments and security departments of the government, and other such agencies and individual forums to deter such attacks and offenders. According to an Australian survey by AusCERT, it was found that 98% of online companies, banks use security software but their employees lack the knowledge of know-how of such software.[25]

Psychological and Emotional Causes: Identity Crisis

With the advent of globalization and modernization, the family structure of all the countries has changed. Particularly in India where the joint family status is most prominent, it was hampered due to the migration of rural people into urban cities in the search for work. This migration has led to the establishment of a single family system due to which privacy and security of their members have become the prime focus. Traditionally, there was a sharing and caring system which has been undone due to nuclear family and work commitments which in turn has led to superficial and insubstantial relationships between their own family members and their neighbours.

Due to work pressure no one has time for anyone even though they may live together. This loneliness of people has led them to socialize and talk on different social networking and dating sites which makes such people more prone to becoming victims of cyber-crimes.[26] In India the ratio of working women is very low compared to men, only 33% of women are engaged in workforce participation in the country whereas men

[23] Duffield & Grabosky, 'The psychology of fraud' [2001] 199 Trends and Issues in Crime and Criminal Justice 1.
[24] Lynch (n 18).
[25]'Australian Computer Crime and Security Survey', (*AusCERT Brisbane* 2004) <http://www.auscert.org.au/crimesurvey>accessed 16 March 2023.
[26] Ravi Krishnani, 'Indian Women: No Friends Online' [2015] 32 World Policy Journal 85.

stand at 67%.[27] Thus, this data indicates that women particularly the home makers are more prone to loneliness, they become aloof because most family members are busy in their professional pursuit and thus chances of women being depressed are higher. Women who stay at home, in particular, have a tendency to look for help outside of their homes to get over despair and loneliness. This is the cause of their propensity to confide in and rely on total strangers.[28]

With technology in their hands and such social networking sites, interaction with strangers becomes easy. To get over this loneliness and fear of missing out, they indulge in chatting, messaging and video calls with not only their known friends but even strangers which releases their catharsis. In such an emotional state, women often become the victim and spell out their secrets and personal information regarding their home, members, property and bank details etc. After receiving such information, miscreants can use such information not only to do cyber-crimes listed above but also heinous sexual crimes.[29]

Illiteracy Vis-À-Vis Digital Illiteracy

India's literacy rate has been improving year by year, though there still exists a gender gap between the literacy rate of men which was 82.4 percent compared to women which was 65.8 percent in 2018.[30] However, out of this proportion of literate people, how many are digitally literate cannot be said. Digital literacy cannot be confined to only using of internet and chatting on Whatsapp , watching videos on YouTube or using Facebook and Instagram but also knowing about terms and condition of the these apps, their privacy policy, data protection norms and protection from virus

[27]Manya Rathore, 'Share of participation at work across India from 2014 to 2023 by gender' (*Statista,* 5 March 2023) <https://www.statista.com/statistics/1043300/india-work-participation-by-gender/> accessed 16 March 2023.

[28] D. Halder & K. Jaishankar, *Cyber Crime and the Victimization of Women: Laws, Rights, and Regulations* (Information Science Reference, IGI Global 2011).

[29] Ibid.

[30] '75 years, 75% literacy: India's long fight against illiteracy' (*Times of India,* 14 August 2022) <https://timesofindia.indiatimes.com/india/75-years-75-literacy-indias-long-fight-against-illiteracy/articleshow/93555770.cms> accessed 16 March 2023.

likes tracing, bugging, hacking, cookies etc. There is a rapid increase in the number of internet and mobile users but severe lack of digital literacy.[31]

There have been many researches done to investigate the impact of gender on computer knowledge and literacy, to the extent that results have shown that males have more computer knowledge than females. An author studied the effect of gender variations in computer mindset and self-efficacy[32]. According to this research, gender inequalities were more pronounced when it came to difficult computer tasks. Regarding elementary computer tasks, there were no discernible differences identified.[33] Males had substantially larger expectations about their own productivity than females did and in comparison to female students, male students indicated less technology fear and more computer confidence.[34] Cultural connotations like patriarchy, misogyny and manhandling could be reasons to explain such results. However, victimization of both men and women on social media platforms is due to their own negligence and lack of interest in knowing and adapting to the latest technology to protect themselves. One can have many options to protect herself or himself from online harassment, trolling, hacking and bullying just by adopting security measures like locking their profile pictures, blocking offenders and reporting them, going for private accounts, and not interacting with unknown persons.[35]

Knowledge of legal rights and awareness to go to the required forum whenever such crimes occur is also lacking. In a research conducted many were found to be not aware about their rights and laws in such cases. Out of 73 respondents, only 80.8% were found to know that hacking, producing and disseminating pornography, disseminating obscene documents, etc. are crimes and 19.2% did not know. Only 19.2% of respondents are aware that their legal right to privacy in cyberspace is subject to penalties, whereas

---

[31] D. Halder & K. Jaishankar, 'Cyber victimization in India: A Baseline Survey Report' [2010] Center for Cyber Victim Counseling.
[32] T. Busch, 'Gender Difference in Self-Efficacy and Attitude towards Computers' [1995] 12 Journal of Educational Computing Research 147.
[33] Ibid.
[34] Ibid.
[35] D. Halder & K. Jaishankar, 'Cyber socializing and victimization of women' [2009] 12(3) Temida 5.

78.1% are aware that cyberbullying, cyberstalking, and sending obtrusive, defamatory texts are all prohibited.[36]

Social roles in the social order cannot be disregarded, notwithstanding the variations in tactics, as they significantly contribute to women's victimization. The connection between gender and digital literacy is influenced by status, traditions, and customs, as well as by age, identity, edification, internet knowledge, income, and race because men predominate because they are skilled computer users and members of global communication networks.[37] They often enforce sexist gender notions in many different ways and anonymity tools act like icing on the cake for such men.

Sociological Reasons: Family Honor, Patriarchal Society

Over the decades, family honour and respectability have lied in the female members of the family. If rape happens, the woman and her family is more victimized by the society than the offender. Society of most nations has been patriarchal in nature. It must have evolved over time but still traces of it can be seen in many different ways. Society's patriarchal nature is a predominant reason for women being victimized by digital crime.[38]

Gender disparities have a significant impact on nurturing behaviours in India. A girl child is supposed to be timid and obedient, whereas a male youngster is taught to be strong and tough. For fear of stigma, women are trained to suppress their voices. Due to such nature and behavioural practices, whenever such crime occurs to them they try to hide such things from the family members and often family members also try to shun their voices.

[36] Ibid.
[37] N. Döring, 'Feminist views of cybersex: Victimization, liberation, and empowerment' [2000] 3(5) Cyber Psychology & Behavior 863.
[38] Halder (n 28).

In a research, Jaishankar and Halder talk about secondary victimization of women which is caused by gender stereotype cyber harassment.[39] The authors describe the process which begins "after the victim begins interacting with reporting agencies, her family and friends and society as a whole".[40] Often the victim shies away from going to the police to preserve her family honour which gives the offender more chances to commit the same crime again and again even to the same person.

According to a report on reporting of cyber-crimes by an NGO Center for Cyber Victim Counseling under which 73 people were taken out of which 60 were women and 13 men. These respondents, who come from various regions of India, are technologically adept, have had some computer expertise, and even utilize social networking websites to hang out in the digital world. They have experienced many forms of victimisation, like receiving threatening emails with sexually explicit attachments, having their profiles hacked, etc. However, not every one of the 60 female respondents has responded. According to the poll, just 35% of the women claimed to be victims, 46.7% did not report, and 18.3% were oblivious to the fact that they had been assaulted. This study demonstrates that, due to social difficulties, women prefer not to report their victimization.

Cyber Addiction and Outlooking Behaviour

The Internet has become a part of our life. Our lives and our routine are motivated by the internet and its behaviour. We have become addicted to it. It may be termed as internet addiction or social networking addiction. The Internet has made so many vloggers and bloggers all over the world. It has given fuel to many lives out there, that it starts dominating their mind, feelings, thoughts etc. Why do we post and share on social networking sites? When we don't like others prying into our life and its privacy then what drives us to post and show everyone, this guided behaviour can be called "internet guided behaviour".

---

[39] D. Halder & K. Jaishankar, 'Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of US, UK and India' [2011a] 6(4) Victims and Offenders 386.
[40] Ibid.

According to an internet critic there are basically five type of internet addiction - web surfing, online shopping, sexual addiction like online relationships, watching porn sites and playing computer games.[41] For many, the internet offers what they can't do in real life - as an escape due to fake accounts and anonymity tools. They make their own identity and act in ways that are not real.

Reasons behind internet addiction is firstly due to its easy availability which gives users a way to either use as boon or bane. Second, is its importance in every task that we do. For example, we are now addicted to WhatsApp and even if we want to leave it we don't see any options because most offices and social groups send their documents, work and updates on it. The third reason for internet addiction can be its availability and affordability - the more the users the cheaper it gets.[42] In India, the whole dynamics of internet affordability was changed by Reliance Jio Telecommunications. Fourthly, the freedom to choose any username and the accompanying anonymity, hides one's real identity due to which whenever communication takes place between online persons and users, it's quite open and frank which builds online relationships more easily. Messenger apps and other dating apps are the creation of this phenomenon.[43]

People initially engage in online communication in an effort to alleviate social isolation, as we have seen earlier in this paper, but eventually they develop an obsession with the virtual realm of the net. The Internet gives addicts a chance to escape the pressures and stresses of daily life. Some people find it difficult to communicate their thoughts in front of others, but they speak more freely about their emotions to his online buddies.[44] Additionally, online interactions have evolved into socially acceptable practices over time. People are now addicted to the internet due to a combination of these elements, and this addiction motivates them to abuse technology.

---

[41] K.S. Young, 'Internet addiction: evaluation and treatment' [1999] 7 Student British Medical Journal 394
[42] M. Temmel, M. Theuermann, E. Ukowitz & T. Vogrin, 'The Impact of the Internet on our daily life' [2001] <https://www.tru.ca/cpj/essay.html> accessed 16 March 2023.
[43] M. D. Griffiths, 'Internet abuse and internet addiction in the workplace' [2010] 22(7) Journal of Workplace Learning 463.
[44]Tanaya Saha & Akancha Srivastava, 'Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization' [2014] 8 International Journal of Cyber Criminology.

Due to easy availability of internet and its frank open communication and no real identity, it offers open sexual communication. Also, there are so many dating apps where one can drive their sexual satisfaction through many ways. Griffith explains such relationships in three different types: the first kind of relationship is typically between strangers who enjoy having sex via the Internet.[45] The duration of this type of relationship is typically brief, and the online lovers may already be married in the real world. Many times, they do not view their online sexual relationships as betraying their marriages. The second category consists of individuals who initially connect online but ultimately decide to continue their connection offline through in-person encounters, letter and gift exchanges, etc.[46] The final type of online relationship involves people who meet online but choose to keep their connection private for years because they may be geographically separated from one another and only occasionally cross paths. Because both parties need to be able to support their relationship financially, this kind of relationship is the hardest to keep up.[47]

Miscreants' outlook towards many apps and their causes show that they choose to outlook for the consequences of what might happen to them. We know of how different apps are sharing data with other companies but even then, as a user choose to use and even depend heavily on it. When we know the consequences of an online public profile, then also we choose to do it and post regularly on it. So many times we overlook the consequences because our behaviour are determined by the internet and its resources which are virtual and we face the consequences of it in the real world.

Social Media Platforms an Easy Getaway to Victimization

We all live in the world of the internet and we use the internet and social media platforms like Facebook, Instagram, Twitter and others in our daily routine. We have become addicted to these sites without which our day cannot pass. Even if we click a picture, that is posted online on different media platforms which not only take data for

[45]M.D. Griffiths, 'All but connected (Online relationships)' [1999] 17 Psychology Post 6.
[46]Ibid.
[47]Ibid.

improvisation of their app but also for other purposes. These platforms and dating sites offer many options to their users to protect their own privacy and account and block users and report them, but many times victims rarely report about such offenders due to many reasons as we have seen above[48]. These sites offer protection to their user but there are many ways in which it itself cannot control what is shared, said and other fake accounts that have been created for crimes like bullying, trolling and cyber misogyny etc.[49] until such accounts and crime are reported. Sites do not have any way to find out such crimes happening on their platforms.

Influencers and bloggers often post their daily life routine in pictures and stories and make videos that are shared via public profile on such social media platforms that can be viewed by the world at large. Such pictures are easily available and can be used for morphing images and can be shared on media platforms and victims can be harassed for such crimes and even extortion can take place.[50] Victims, to save their reputation, often do not complain and are caught in this web of crimes. Many a time due to stories of these bloggers the offender can know all the things and when such a person is available and what time is perfect to commit any crime against him.

INDIAN CYBER LAWS: A PROSPECTIVE ANALYSIS

After the World War was over, many people became victimized by the grave crimes that occurred during those years. In earlier days crimes were only physical in nature like terrorism, human rights crimes, war crimes etc. Later, in the era of 70s and 80s, with the emergence of computer and telecommunication technologies, crimes started taking place in society which were not physical and limited to a geographical and sovereign region of one country. All over the world, academicians, scholars and

[48] Tom van Laer, 'The Means to Justify the End: Combating Cyber Harassment in Social Media Source' [2014] 123 Journal of Business Ethics 85.
[49] Kim Barker & Olga Jurasz, 'Dynamics of Global Feminism' [2019] 72 Journal of International Affairs 95.
[50] Mary Banach, 'Victimization Online: The down Side of Seeking Human Services for Women on the Internet' [2000] Cyber psychology & behavior: The Impact of the Internet, multimedia and virtual reality on behavior and society.

computer specialists were engaged in defining cyber-crimes, how computer attacks can be done and how it can be limited. No bill, regulation and laws of any country had cyber-crime listed in it, and there was no uniformity in anyone's thoughts on how to provide a uniform definition of it.[51] Computer crimes were defined by the Department of Justice, US as those crimes where "knowledge of a computer system is essential to commit the crime."[52] In the initial period "cyber-crime" was categorized in two parts, firstly was attack on machines and second category was computer assisted crimes done through different mediums.[53]

Cybercrime can occur in the first scenario when computer files and programs are accessed or disturbed without authorization, or when a user's digital identification is stolen.[54] The second instance of cyber-attacks is when a technology is used to carry out more conventional crimes, such as the production or distribution of child pornography, the commission of economic crime, the reproduction of well-known music that are protected by copyrights, etc.[55] Nevertheless, these definitions demonstrate that the phrase "cyber-crime" refers to any crime committed with the use of the internet.

In the Convention of Prevention of Crime and Treatment of Offenders which was held in Vienna by the United Nations in the year 2000, the need to have a definite law and universal preventive measures for cyber-crime was felt. The idea of this convention was further strengthened by the creation of the "Convention of Cybercrime" by the European Council held in Hungary in the year 2001. This convention gave cybercrime five dimensions which are firstly crimes against the secrecy, integrity of computer data and its systems; secondly computer-related crimes; thirdly content related crime; fourthly crime relating to infringement of copyright and the fifth dimension was abetment and aiding of such crimes.[56] In this convention, individual attack by cyber-crime was not recognised - the definitions only mentioned the machine attacks by or

---

[51] D. S. Wall, 'The Internet as a conduit for criminals' [2005] Information Technology and the Criminal Justice System 77.
[52] D. B. Parker, 'Computer crime: Criminal justice resource manual' [1989] Department of Justice, National Institute of Justice.
[53] N. K. Katyal, 'Criminal law in cyberspace' [2001] University of Pennsylvania Law Review 149.
[54] Ibid.
[55] Ibid.
[56] Council of Europe, 'Convention on cybercrime', Budapest (2001) <https://www.coe.int/en/web/cybercrime/the-budapest-convention> accessed 16 March 2023.

through computer operated machine but now as we see the computer and vast internet are just tools of cyber-crime which offers motive to the offender to ruin the reputation of the victim through different types of crime against any person. Earlier conventions and laws of nations were merely drafted for the protection of e-commerce sites and not to protect an individual person and his privacy in the realm of the internet world.

Lacuna and the Effectiveness

India has the Information and Technology Act, 2000. India's law had been made only to protect e-commerce and financial institutions from the attacks of cyber-crimes. It doesn't talk about the individual effect of protection of women, men and children from personal attacks that could occur to them in the digital world. In India, "Internet crime against women" is a problem that few discussed or attempted to address which left countless victims suffering in silence. According to the Information Technology Act of 2000, the term "cyber-crime against women" is most commonly used to refer to sexual offences and online sex abuse, such as altering images for pornographic purposes, harassing women through sexually explicit emails or texts, or cyberstalking.[57] That is why the Indian IT act did contain one section which covered pornography and obscenity in the internet which is section 67 of the act in which most of the earlier cases were booked in. However, India did have a central law like the Indecent Representation of Women (Prohibition) Act, 1986 and Indian Penal Code sections like 509, 292 and others which were invoked from time to time to protect women from such indecent crimes but in today's era such sections have become outdated. The Indecent Representation of Women (Prohibition) Act, 1986 was made especially for women and it prohibited publications and advertisements which contained indecent representations of women. But it has to be noted that the Indian concept of obscenity is way different

[57] K.G.Balakrishnan, *'Speech at seminar on cyber-crimes against women - Public awareness meeting'*, Maharaja College, Ernakulam [2009].

from western concept.[58] Thus, any sexual portrayal of women, or sexual dressing of women in any manner could be considered as obscene by the Indian society.[59]

Feminists insisted upon their protection but they criticised such a law because it mentions crime against women only from the angle of obscenity which attaches a moral standard to it and not mere derogatory aspects of crimes that can be done against women.[60] Thus, this act failed to achieve what it was intended for because the law was a very Indian concept of gendered morality. The Act was to be amended to be on par with the punishment prescribed in the information and technology act and was made to be applied to digital media. If the proposed amendment could have taken place then India could have a law specifically addressing the victimization of women through indecent portrayal is undoubtedly a positive development.

The Indian IT Act was amended in the year 2008 which added section 67A[61] and 67B[62] which is gender neutral and which made the production, creation and distribution of obscene and sexually explicit material in digital form. Section 67 and 67A together are helping in defending the cybercrimes against women that are happening, but these provisions only provide for a charge and monetary damages and punishes "whoever" commits the crime which means even if any indecent picture is produced by the creator himself he can also be held guilty of crime.[63]

The present Indian IT law still has lacunae in it which are ***firstly,*** that the act does not mention about the "removing or deleting of the derogatory matter". When any crime like morphing of pictures has been done by the offender and that image has been circulated on various sites, the traumatic effect which such crimes and that morphed photo can leave on the victim is indispensable. Thus the act should mention the

---

[58] Halder, Debarati, 'Examining the Scope of Indecent Representation of Women (Prevention) Act, 1986, in the Light of Cyber Victimisation of Women in India' [2013] 11 National Law School Journal.
[59] Geetanjali Gangoli, *Indian feminisms: Law Patriarchies and violence in India* (Ashgate Publishing, Ltd. 2012).
[60] Vedkumari, 'Gender Analysis of the Indian Penal Code' in Archana Parashar & Amita Dhanda (eds), *Engendering law: Essays in honor of Lotika Sarkar* (EBC 1999).
[61] The Information Technology Act, 2000.
[62] Ibid.
[63] Haldar (n 60).

protection of the victims and other means by deleting such pictures, blocking accounts etc. from all over the internet.

Secondly, the IT act does not mention women investigating officers or reporting cyber cells exclusively for women. It is regrettable to see that the current Act makes no mention of gender-specific victim assistance cells. In some circumstances, neither Section 78 of the I.T. Act, 2000 nor Section 80(1) clearly state whether a male or female officer is qualified to conduct an investigation, conduct a search, or make an arrest.[64] The low reporting of crime is a sign that female victims are facing social stigma and they fear the dreadful police station and men police officers out of their fear of social reputation. Thus, women police officers specially equipped with knowledge to deal with cyber-attacks must be appointed.

Thirdly, Indian IT act mentions the term “whoever commits” which means that if the original profile creators themselves create, publish, or transmit images that reveal too much skin or conduct that is considered "sexually explicit" or "obscene" in orthodox societies like India. Thus, the language of this section could be interpreted to apply to even the original profile creators. Because of this, authorities frequently accuse victims of being 'too attractive' in their attire, which would have encouraged the offender to perpetrate the crime while wearing a similar appearance.

Fourthly, the internet service provider companies and the other intermediaries need to be more accountable. All the crimes are committed on the internet are hosted by different sites like Google, Yahoo, Facebook etc. We observe that many Indians sign up for social media platforms based in the US, create accounts with US-based ISPs, or participate in online chat rooms that follow US laws and regulations. The victims of victimization on these sites frequently witness "odd responses" from the ISPs in addition to the legal and judicial systems.[65] This is due to the fact that either such victimization does not meet the criteria for crimes under the ISPs' policy guidelines or it is not considered illegal under Indian law. The accountability of such sites needs to be more rigid whenever such crimes occur. Privacy of data is also one of the major concerns

[64] Cox (n 10),
[65] Halder (n 28),

these days which all the apps and sites are taking from the individuals itself, and when such data is shared with other companies without permission from the individual it creates an environment where crime can be done and specific persons and institutions can be targeted with it. As India does not have any Data Privacy Law such provision needs to be valued from a future perspective.

Fifthly, there is no uniformity in laws of all the countries and no universal international cyber law to protect all the victims and punish the offenders. As we know that in the global world email, sites, apps can be operated from anywhere in the world, as does the crime which takes place on such sites and the offender could be anywhere in the world and commit a crime in India and roam freely because there is no legislation to bring such criminals from different countries and make them accountable for what they did. Cyber-attacks cannot be confined to regional laws thus it needs international cyber laws when such a situation occurs. When foreign websites are contributing to crimes against not only women but all persons and institutions, companies in India, problems about the proper application of the law also come up.[66]

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: A step towards more inclusive, safe and accountable cyberspace

To help make cyberspace safe, trusted and accountable, the Central Government, in exercise of powers conferred by the IT Act, has made the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which require intermediaries, including social media intermediaries, to observe, among others, diligence as under:[67]

- To publish on their website and app, their rules and regulations, privacy policy and user agreement;
- To inform the said rules to their users and to make reasonable efforts to cause the users not to host, display, upload, modify, publish, transmit, store, update or

[66] Ibid.
[67] Cybercrime Against Women, <https://pib.gov.in/PressReleseDetailm.aspx?PRID=1881404> accessed 10 July 2023.

share, among others, information which belongs to another person, or is obscene, or is invasive of another's privacy, or is insulting or harassing on the basis of gender, or is racially or ethnically objectionable, or encourages money laundering, or promotes enmity between different groups on the grounds of religion or caste with the intent to incite violence, or is harmful to child, or infringes intellectual property rights, or impersonates another person, or threatens the unity, integrity, defence, security or sovereignty of India or public order, or prevents investigation, or violates any law;

- Upon receipt of an order from a lawfully authorised government agency, to provide information or assistance for prevention, detection, investigation or prosecution under law, or for cyber security incidents;
- To have in place a grievance redressal machinery, and resolve complaints of violation of the rules within 72 hours of being reported;
- In case an intermediary is a significant social media intermediary (i.e., an intermediary having more than 50 lakh registered users in India), to additionally observe due diligence in terms of appointing a Chief Compliance Officer, a nodal contact person for 24x7 coordination with law enforcement agencies and a Resident Grievance Officer, publishing monthly compliance reports, etc.

Further, it has notified amendments to these rules on 28.10.2022 to provide for the establishment of one or more Grievance Appellate Committee(s) to allow users to appeal against decisions taken by Grievance Officers on such complaints. In addition, the Ministry of Home Affairs operates a National Cyber Crime Reporting Portal to enable citizens to report complaints pertaining to all types of cybercrimes, with special focus on cybercrimes against women.[68]

CONCLUSION

The Internet has the ability to empower everyone at the start of the new millennium by providing them with access to knowledge and social support regarding

[68] Ibid.

their concerns about their physical and mental health as well as by promoting digital advocacy for shifts in societal and organizational policy. However, there are dangers and potential dangers that must be addressed. Online victimization can be brought on by incomplete information, invasion of privacy, restricted communication, online harassment, and cyberstalking. If the potential of the Internet to deliver services is to be realized, users both individuals and other institutions and e-commerce sites must comprehend and protect against these risks. Taking precaution and education about online safety and privacy issues are important but not the end. Laws of a nation often reflect its social and moral values and have social conduct rules. Over the years technological advancement has taken up with a rapid speed and has increased the number of users of the internet, computer and mobile phones, it has changed faster than the laws governing them. It has created a wave of opportunities for many people, but it's often a curse for many who have been victimized by it in any form.

Cyber-crimes are immoral and can harm the reputation of victims to a great extent but many countries only recognise the sexual aspect of such cyber-crimes against women particularly and do not value cyber-crimes of non-sexual types. Countries still need to move away from the social aspect of laws that are framed to combat such crimes and give proper protection. Due to fear of reputation and other social stigma attached to their family such crimes are often less recognised and reported out in the public. There is a lack of awareness on the part of the public as well as investigating officers and cyber cells. They often don't know how to react and act when such incidents have taken place and victim comes for help. We recognise that the primary cause of the low reporting rates and nearly nonexistent use of the laws intended to address offences other than obscenity and pornography is a lack of understanding among the general public, particularly among female victims.

Laws often just prescribe punishment like imprisonment, fine or damages to the victim. The law should look beyond this. They should be looking out for victim welfare and how to resynthesize them back in society if they have been suffering from the trauma of cyber-crimes. The police officer or the cyber cell or trial judge could do much more by ordering the removal of the online material posted or shared by anyone without

such person’s consent. Police officers should be given training to handle such cases and there should be cyber cell officers in every police station. There should be cyber hotlines for sharing such grievances. Reputation management techniques and modal conduct should be taught which can help victims overcome his fear.

Furthermore, it must be kept in mind that cyber victimization cannot be stopped by simply imposing fines or jail terms as penalties. When it comes to tracking subscriber usage by generating new identities and using social media or other web platforms to further harass the victims. Online service providers like Whatsapp, Google, Yahoo, Facebook, Instagram and Twitter, which are actually based in the US, are almost completely irresponsible when it comes to tracking subscribers' online activity through the creation of false identities and the use of social media or other websites to harass victims even more. People and students must be given general training and know how to use such apps and software for protecting them from such crimes and reporting them to the requisite authorities.

Thus the internet is a boon or bane that depends on how one uses it. It may offer endless opportunity and attraction but one must always be aware of their rights and privacy and know how to use such apps and technologies in the greatest positive manner.