

# An Empirical Study on Cyber Crimes Against Women in India

K. Sarunisha<sup>1</sup> and Ms. Ambika Bhat<sup>2</sup>

B.A.Llb (Hons), Saveetha School of Law<sup>1</sup>

Assistant Professor, Saveetha School of Law<sup>2</sup>

Saveetha Institute of Medical and Technical Sciences (SIMATS), Saveetha University, Chennai, India

**Abstract:** *In general cyber crime may be defined as “ Any unlawful act where a computer or communication device or computer network is used to commit or grease the commission of crime ”. People were forced to use the internet for educational, rest, professional, and social purposes throughout the epidemic and lockdown. Working women began working from home using laptops, smart- phones, and the web. Women who are still enrolled in academy have been forced to use the web for online literacy and other educational conditioning. Due to the fact that the maturity of women were using social media websites and one or further online platforms for educational, occupational, and recreational purposes during this time period, the rate of cybercrime against women began to rise. This is an empirical study on cyber crimes against women in India. Both Men and women are victims of cyber crime but women are more in rate. As a result it's hard to put a crime-free society that's insolvable to achieve and only exists in fantasy, it should be a continuing trouble to apply regulations that reduce crime to a minimum. Particularly in an decreasingly technologically reliant world, crime related to electronic law- breaking is certain to increase, and lawmakers must go the redundant afar to keep hoaxers atbay. The experimenter has followed the empirical exploration with the accessible slice system. The sample size covered by the experimenter is 201. The results observed from the empirical study on cyber crime against women in India. The conclusion indicated that To combat cybercrime against women, the Legal system has legislated a number of legislation.*

**Keywords:** Cyber crime, Network, women, Crime, Legislator.

## I. INTRODUCTION

Information Technology results have paved a way to a new world of internet, business networking and e-banking, expiring as a result to reduce costs, change the sophisticated profitable affairs to an easier, speedy, effective, and time saving system of deals. colorful culprits like hackers, crackers have also set up ways and measures to intrude with the internet accounts and have been successful in gaining unauthorized access to the stoner's computer system and stolen useful data. The computer- generated terrain of the internet is pertained to as cyberspace, and the rules that govern it are pertained to as cyber laws. All druggies of this space are subject to these laws, as it carries a kind of global governance. It involves following a person's movements across the Internet by posting dispatches( occasionally hanging ) on the bulletin boards visited by the victim, entering the converse- apartments visited by the victim, constantly bombarding the victim with emails etc. In general, the snooper intends to beget emotional torture and has no licit purpose to hiscommunications. Cyber vilification Cyber vilification also called Cyber smearing can be understood as the purposeful violation of ‘ another person's right to his good name. ‘ Cyber Defamation occurs with the help of computers and/ or the Internet. It's considered further of an imminence owing to its ready nature. therefore, cyber-crime might be defined as a conflation of crime and technology. To put it simply, ‘ any offence or crime that involves the use of a computer is a cyber-crime. ’ Cybercrime refers to crimes committed over the internet in which the perpetrator, hidden by the curtain of a computer screen, isn't needed to make particular contact with another person and may not always expose their name. In a cyber-crime, the computer or the data is the target, the thing of the offence, or a tool used to commit another offence by furnishing the necessary inputs. All of these types of offences fall under the broader term of cybercrime. Cyber bullying A form of importunity or bullying foisted through the use of electronic or communication

bias similar as computer, mobile phone, laptop, etc. The remedies In case of cyber- crimes, a victim may communicate the nearest cyber cell or police station. A complaint may also be filed anonymously through National Cyber crime Reporting Portal( cybercrime.gov.in).The rapid technological advancements like the internet clearly threaten to leave the law behind. The open and unregulated nature of the internet and the irrelevance of geography means that the internet also provides futile ground for criminal enterprise. The existing criminal law seems to be ill equipped to deal with this up-gradation in methods and media of committing crime. Cyber-crime has thus become a reality in India, difficult to detect, seldom reported and even difficult to prove. Computer related crime lacks a traditional paper audit, is away from conventional policing and requires specialists with a sound understanding of computer technology. Paperless contracts, digital signatures, online transactions and cyber crimes have taken the legal world by surprise. Traditional laws formulated to govern the simple and less criminal world are dumb and toothless. Evidence, the foundation stone of the great legal edifice suffers jolt. The biggest blow is given by lack of visual evidence. The internet matrix has disturbed the legal ambiance whereas the legal provisions are chasing the cyber criminals who are resorting to new modus operandi now and then.

**Ritu Kohli's Case:** For the purposes of this section, terms “Electronic mail” and “Electronic Mail Message” means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.”Likewise the Indian Parliament made amendments to the Indian Penal Code, 1860 introducing cyber stalking as a criminal offense. The Criminal Law (Amendment) Act 2013 added Section 354 D in IPC, 1860. It defines Stalking as a man who follows or contacts a woman, despite clear indication of disinterest to such contact by that woman, or monitoring the use of the internet or electronic communication of a woman.

A man or a woman committing the offense of stalking would be liable for imprisonment up to three years for the first offense, and shall also be liable to fine and for any subsequent conviction would be liable for imprisonment up to five years and with fine.

### 1.1 OBJECTIVE

- To examine the various forms of cyber crimes against women in India.
- To analyze the information on current trends on cyber crimes against women in India.
- To suggest some legal and interesting measures regarding cyber crimes against women in India.
- To give awareness to general public about the laws enacted for cyber crimes against women in India

## II. LITERATURE REVIEW

The computer-generated environment of the internet is referred to as cyberspace, and the rules that govern it are referred to as cyber laws. All users of this space are subject to these laws, as it carries a sort of global jurisdiction. Additionally, cyber law can be regarded as a branch of law which deals with legal issues arising from the use of networked information technology.<sup>1</sup>

**Purnima Ojha** The Indian Journal of Political Science Women may have stardom in any stream but are getting harassed every day by their surroundings. They are victims of crime mostly including directly specified cyber crimes, rape, kidnapping and abduction, dowry- related crimes, molestation, dge1.tn.nic.in sexual.<sup>2</sup>

**Jacqueline D. Lipton Berkeley** Technology Law Journal Gender based crimes are those crimes committed against persons, whether male or female, because of their sex and/or socially constructed gender roles<sup>3</sup>

**Kim Barker, Olga Jurasz** Crimes that are a form of gender-based cyberviolence include: online hate speech, trolling, cyber harassment, cyberstalking, sharing content without consent, hacking, identity theft, cyberbullying, and image-based sexual abuse.<sup>4</sup>

**Phillip Pool** The International Lawyer Cyber violence against women can be defined as any form of gender-based and sexual violence expressed through ICTs such as the Internet, mobile phones and video games<sup>1</sup>. Many features of these technologies make them ideal weapons for committing gender violence.<sup>5</sup>

**Loubna H. Skalli** Journal of Middle East Women's Studies, Vol. 2, No. 2, Special Issue: Women's Activism and the Public Sphere (Spring 2006), form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc. Cyber grooming.<sup>6</sup>

**Danielle Keats Citron Michigan** Law Review, Vol. 108, No. 3 (Dec., 2009), Stalkers are strengthened by the anonymity the internet offers. He may be on the other side of the earth, or a next door neighbor or a near relative! It involves following a person's movements across the Internet by posting messages<sup>6,7</sup>

**Tom van Laer** Journal of Business Ethics Cyber defamation also called Cyber smearing can be understood as the intentional infringement of 'another person's right to his good name'<sup>8</sup>

**Mark Austin Walters**, Jessica Tumath The Modern Law Review, Vol. 77, The internet and social media are certainly a great thing for people and society in general, but they are also uniquely effective breeding ground for potentially libellous statements.<sup>9</sup>

**Lisa Sharland**, Genevieve Feely Australian Strategic Policy Institute (Jun. 1, 2019) Email is remarkably quick and easy to use method of correspondence. It has a close resemblance to spoken conversation rather than written interaction<sup>10</sup>

**Kamlesh Vaswani** Nothing can more efficiently destroy a person, fizzle their mind, evaporate their future, eliminate their potential or destroy society like pornography." - Kamlesh Vaswani, Activist<sup>11</sup>

**RAVI KRISHNANI** World Policy Journal, the rate of cybercrime against women began to rise. Due to the fact that the entire country was on lockdown, criminals were unable to physically assault the victim, and thus began mentally and emotionally harassing them.<sup>12</sup>

**Sanjay Goel** Connections Due to the fact that the majority of women were using social media websites and one or more online platforms for educational, occupational, and recreational purposes during this time period<sup>12,13</sup>

**Brandon Gaskew** Third Way Due to the fact that the majority of women were using social media websites and one or more online platforms for educational, occupational, and recreational purposes during this time period it's been advantage to criminals to miss use it<sup>14</sup>

**Shiv Visvanathan** Economic and Political Weekly, SEXTORTION is the most frequently committed cybercrime involving women during the pandemic period. The criminals began extorting or sexual favours from their victims by blackmailing them into disclosing their private photographs or modified images.<sup>15</sup>

**Clay Wilson** From: Cyberpower and National Security, Potomac Books( cyber hacking) People began reading news online during the pandemic. There has been an increase in the number of instances of bogus news and information. The women became victims of cyber hacking after clicking on malware URLs that downloaded all their personal information on their phones, activated the microphone and camera, and captured their intimate photos and videos.<sup>16</sup>

**Gregor Urbas** From: Cyber-Crime: The Challenge in Asia, Hong Kong University Press (2005) Cyber bullying posting false and misleading and abusive statements about the victims on social networking sites land demanding payment to have them removed, leaving hurtful comments on the victim's posts, exchanging morphed/private pictures of the victims without her consent, and sending rape and death threats to the victim, among other things.<sup>16,17</sup>

**William Perdue, Julia Spiegel** California Law Review Throughout the epidemic, perpetrators engaged in online sexual assault of women, morphing the victim's image and utilizing it for pornographic purposes.<sup>18</sup>

**Shawn Henry, Aaron F. Brantly** The Cyber Defense Review To summarize, while a crime-free society is impossible to achieve and only exists in fantasy, it should be a continuing effort to enforce regulations that reduce criminality to a minimum<sup>19</sup>

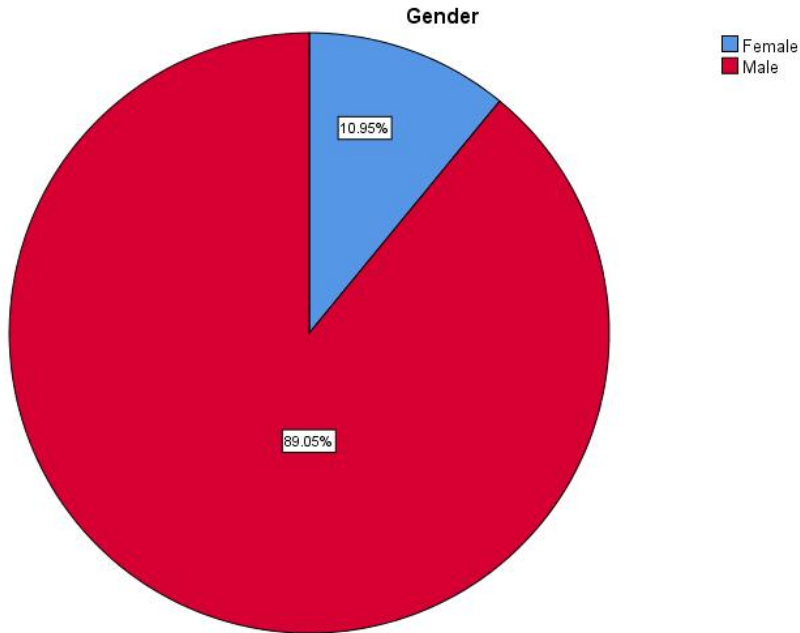
**Kamal T. Jabbour, Erich Devendorf** The Cyber Defense Review, increasingly technologically reliant world, criminality related to electronic law-breaking is certain to increase, and legislators must go the extra mile to keep impostors at bay. Technology is often a double-edged sword that can be employed for either good or evil purposes.<sup>19,20</sup>

### III. METHODOLOGY

The research method followed is empirical research. A total of 201 samples have been taken out of which is taken by a convenient sampling method. The sample frame taken by the researcher through online mode and offline also collected certain responses. The independent variables taken for the survey are age, gender, occupation and educational qualification. The statistical tool used in the study is graphical representation, anova test and chi square analysis.

**IV. ANALYSIS:**

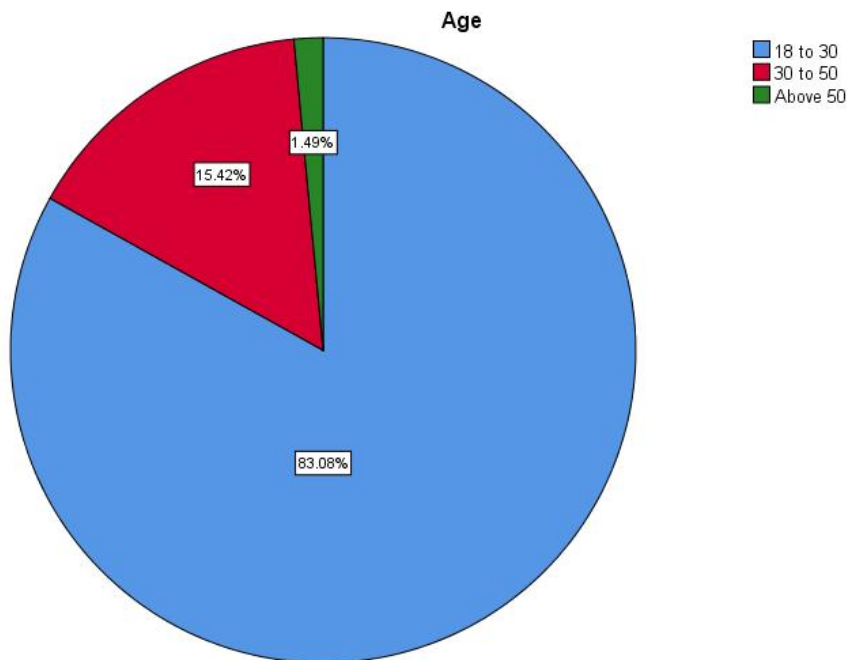
**FIGURE 1: Pie analysis - Gender Response**



**LEGEND:**

In the above pie chart fig 1, we can see that the independent variable gender response have been analyzed in which male have been responded in more number.

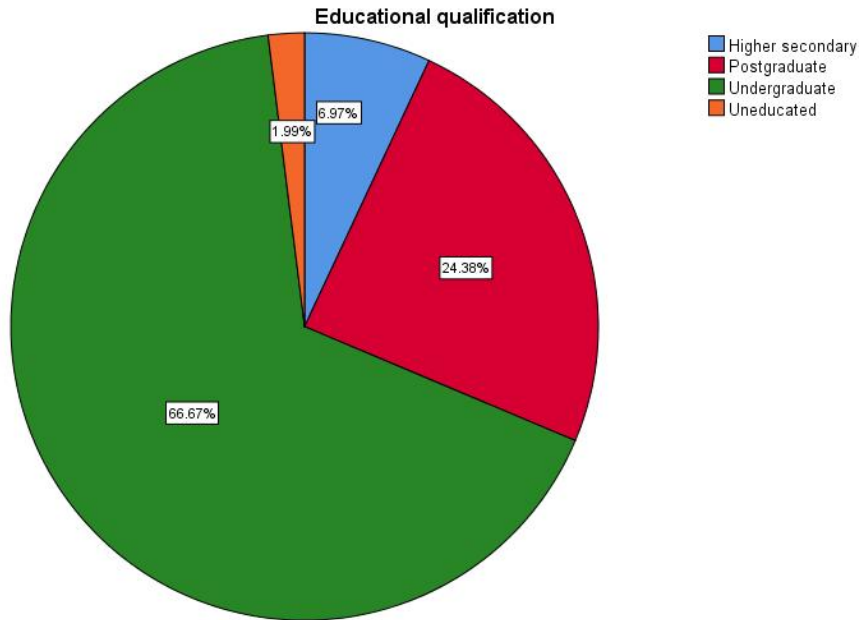
**FIGURE 2: Pie analysis - Age Response**



**LEGEND:**

In the above pie chart fig 2, we can see that the independent variable age response have been analyzed in which 18-30 have been responded in more numbers .

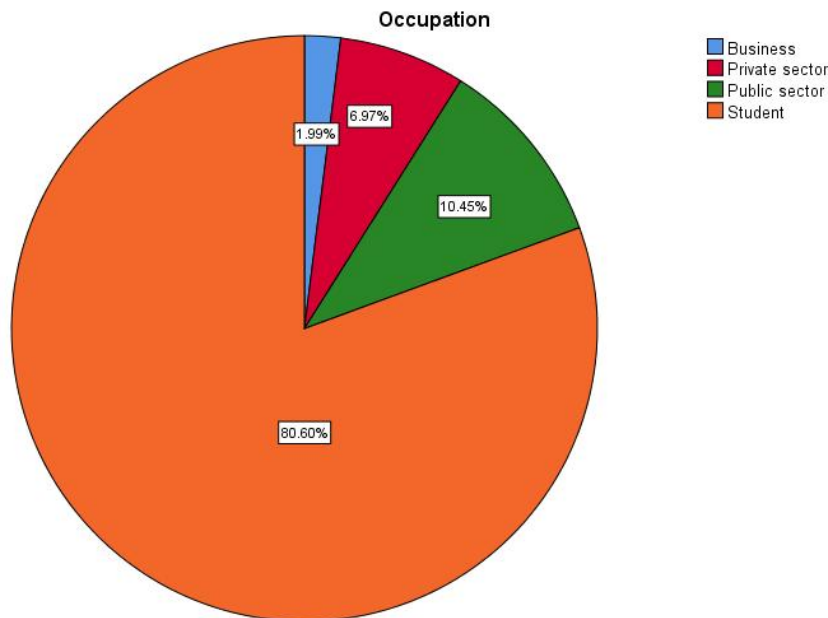
**FIGURE 3: Pie analysis - Education Qualification Response**



**LEGEND:**

In the above pie chart fig 3, we can see that the independent variable educational qualification response is analyzed in which undergraduate has been responded in more number .

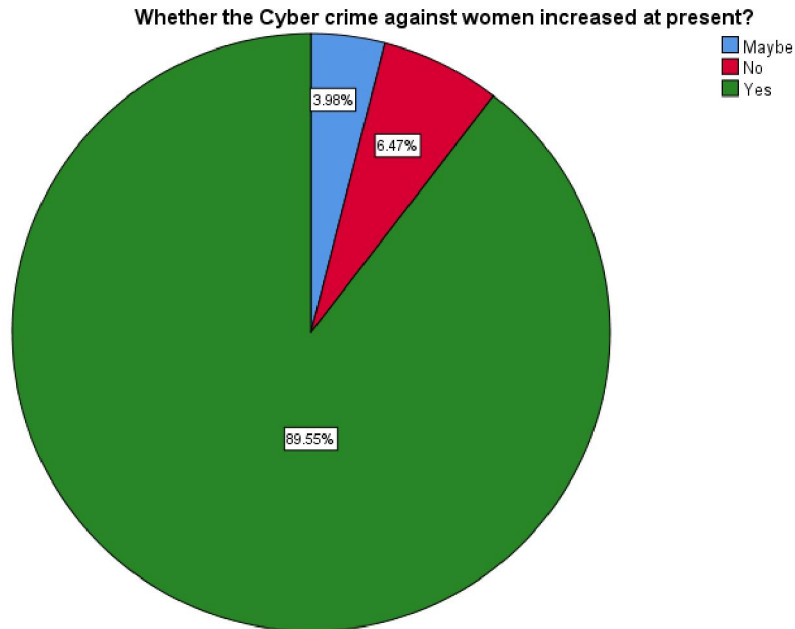
**FIGURE 4: Pie analysis occupation response**



**LEGEND:**

In the above pie chart fig4, we can see that the independent variable occupation response is analyzed in which students has responded in more number .

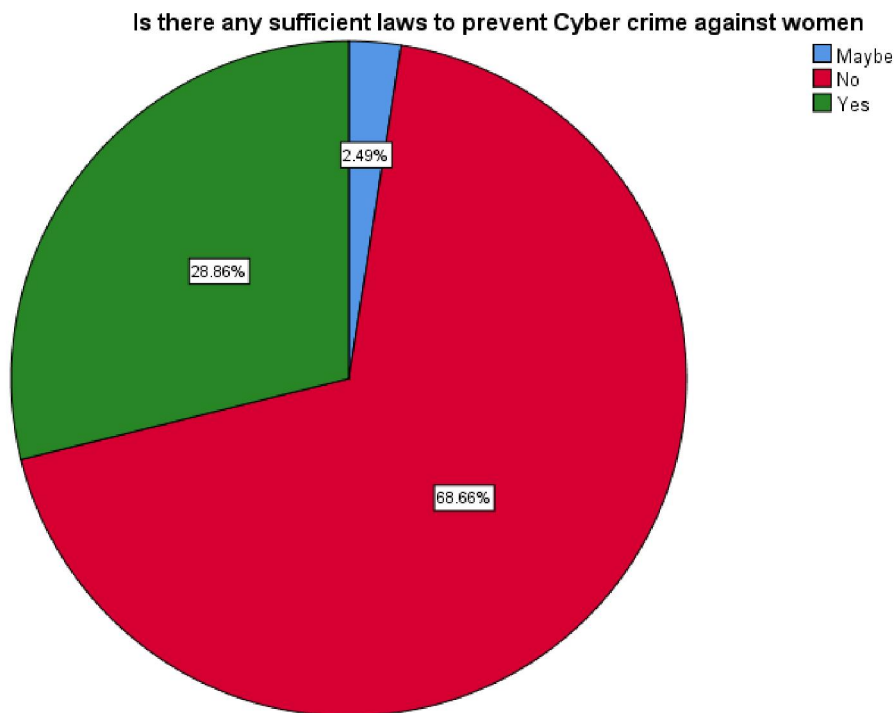
**FIGURE 5:** Pie analysis whether the cyber crime against women increased at present



**LEGEND:**

In the above pie chart fig 5, we can see that the dependent variable whether the cyber crime against women increased at present YES has been responded more.

**FIGURE 6:** Pie analysis - Is there any sufficient laws to prevent cyber crime against women

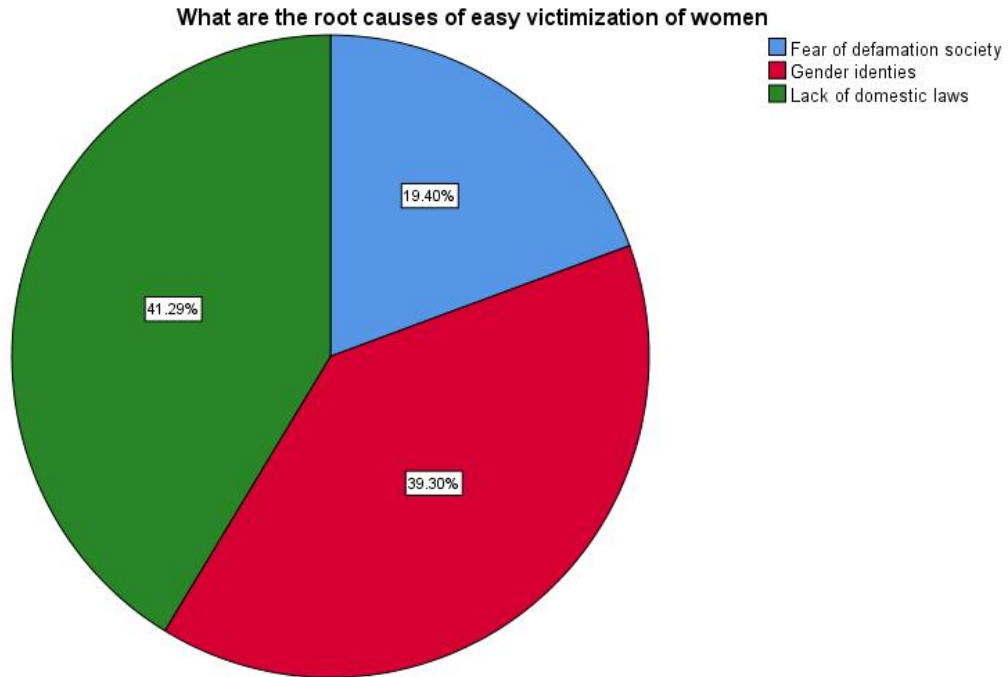




**LEGEND:**

In the above pie chart fig 6, we can see that the dependent variable Is there any sufficient laws to prevent cyber crime against women NOhas been responded more.

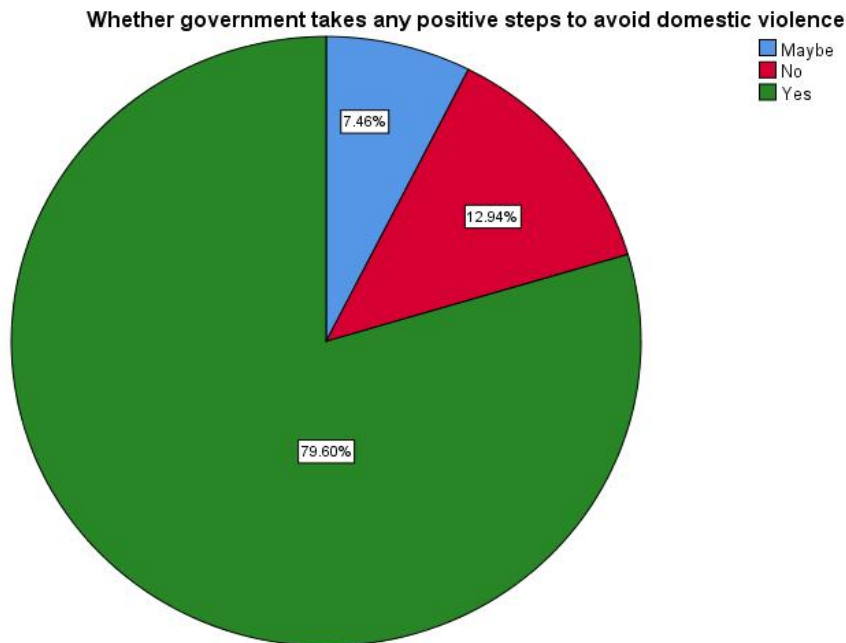
**FIGURE 7:** Pie analysis - what are the root causes of easy victimization of women



**LEGEND:**

In the above pie chart fig 7, we can see that the dependent variable whether the root causes of easy victimization of women lacking domestic loss has been responded more.

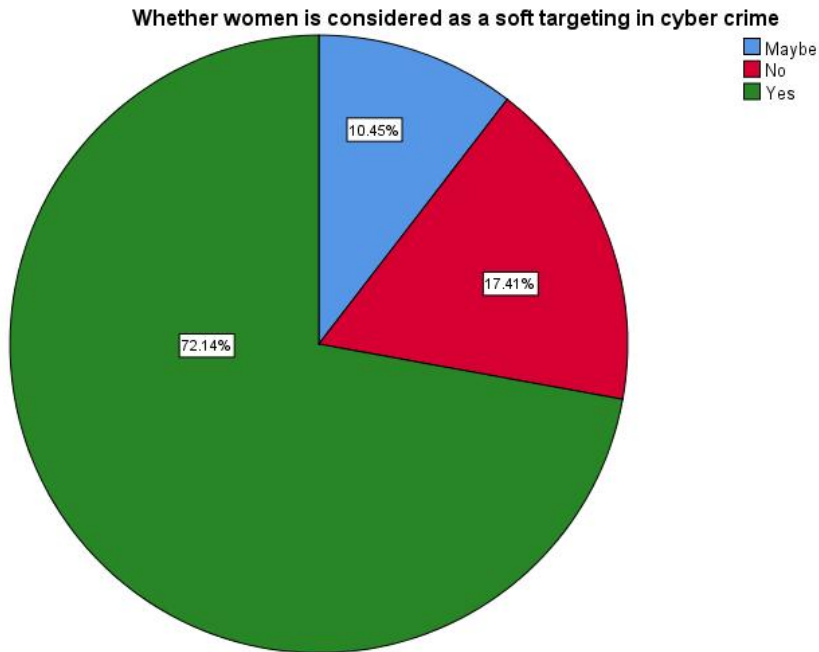
**FIGURE 8:** Pie analysis - whether government takes any positive steps to avoid domestic violence



**LEGEND:**

In the above pie chart fig 8, we can see that the dependent variable whether government takes any positive steps to avoid domestic violence YES has been responded more.

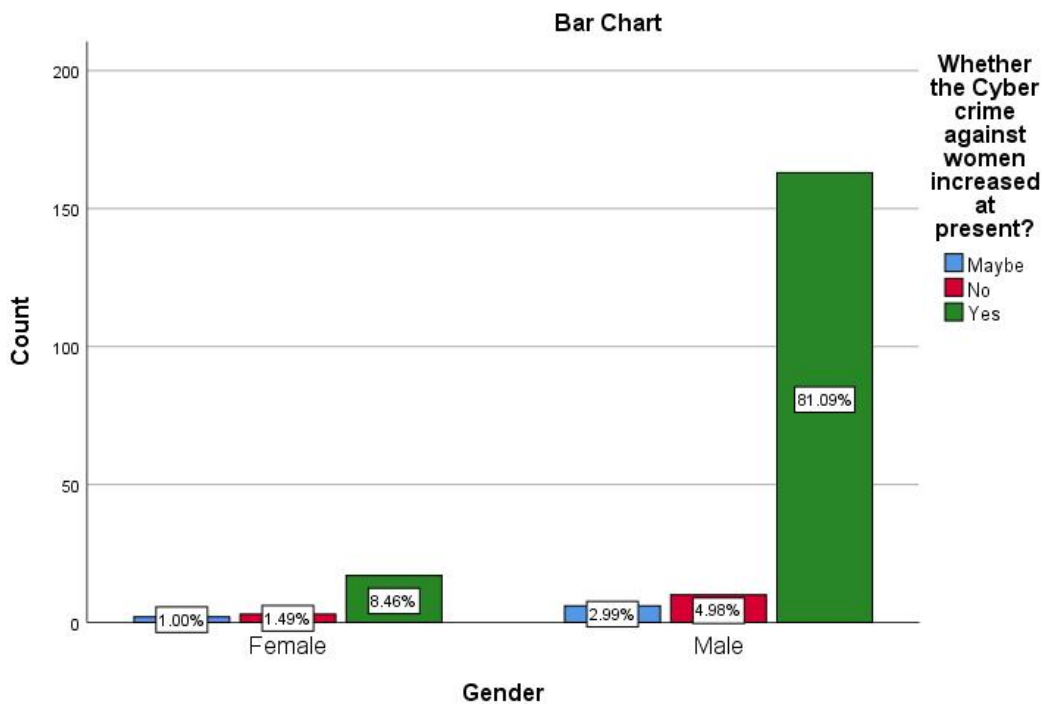
**FIGURE 9:** Pie analysis - Whether women is considered as a soft targeting in cyber crime



**LEGEND:**

In the above pie chart fig 9, we can see that the dependent variable whether women is considered as a soft targeting in cyber crime YES has been responded more.

**FIGURE 10:** GENDER \* Whether the cyber crime against women increased at present ?

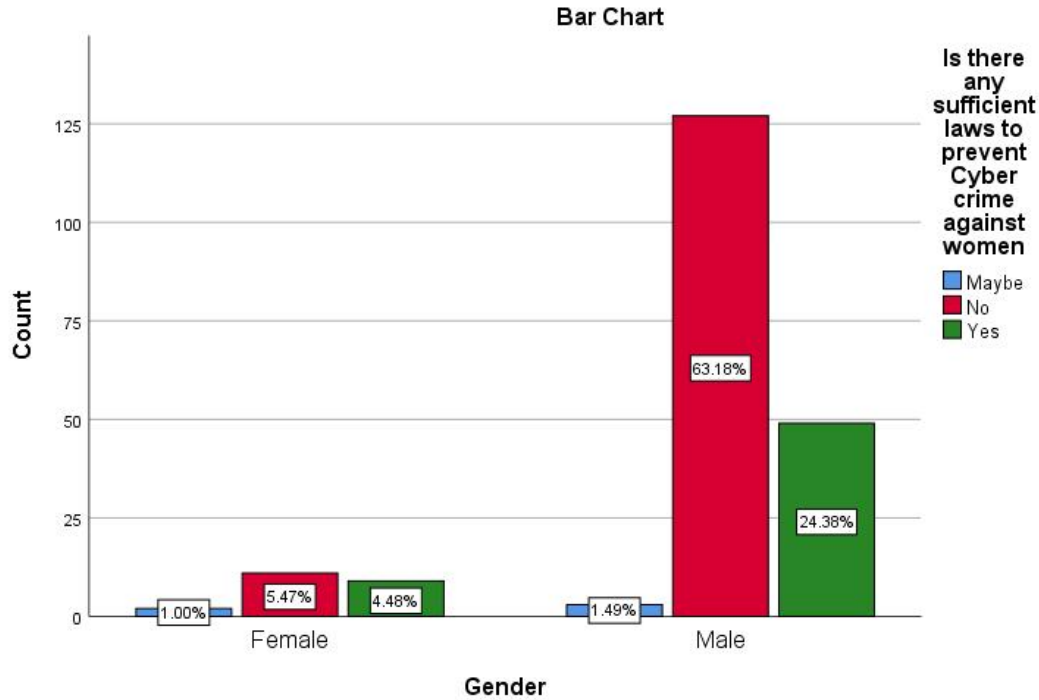




**LEGEND:**

In the above bar chart fig 10, we can see that the dependent variable whether the cyber crime against women increased out of which male has responded more in number stated YES.

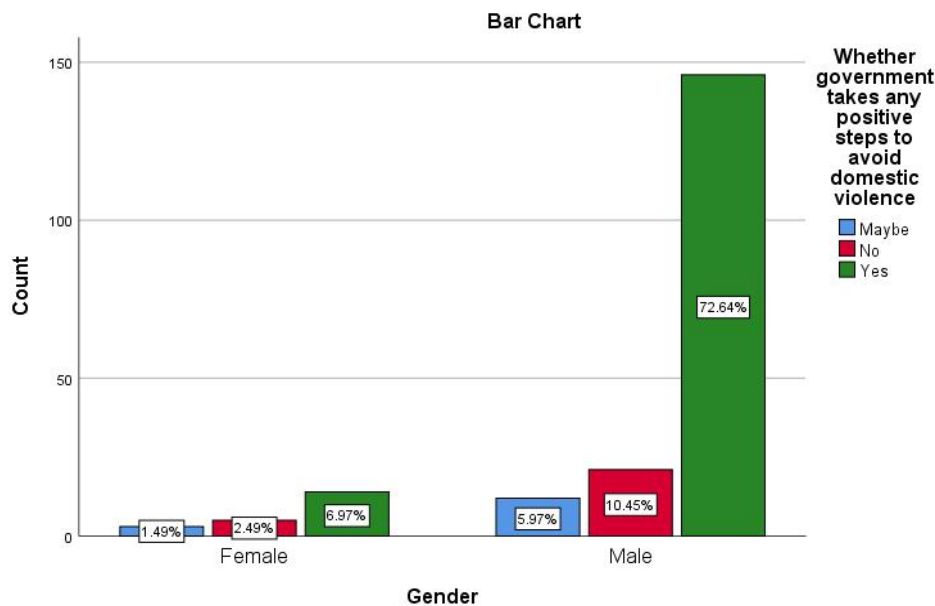
**FIGURE 11: GENDER \* Is there any sufficient laws to prevent cyber crime against women**



**LEGEND:**

In the above barchart fig 11, we can see that the dependent variable Is there any sufficient laws to prevent cyber crime against women out of which male has responded YES in more number.

**FIGURE 12: GENDER \* Whether government takes any positive steps to avoid domestic violence**

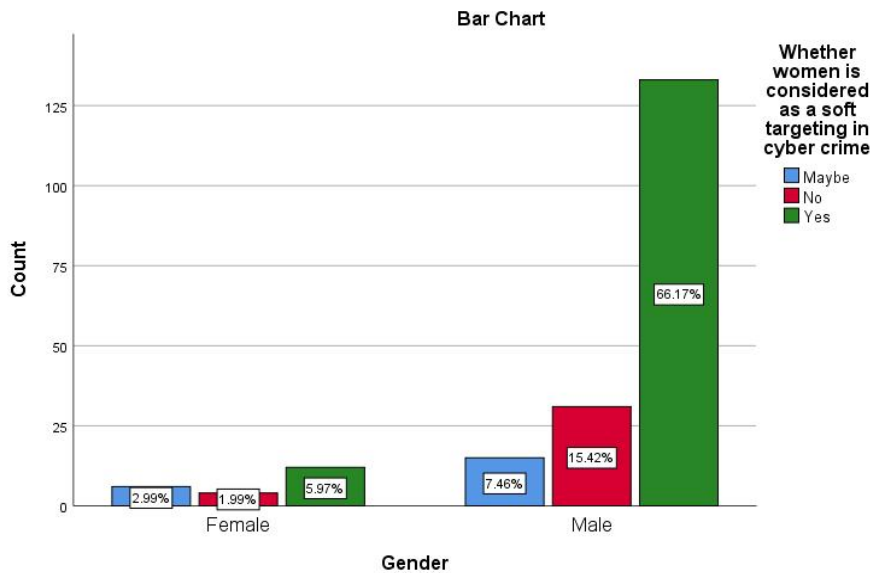


**LEGEND:**

In the above barchart fig 12, we can see that the dependent variable whether government takes any positive steps to avoid domestic violence out of which male has responded YES in more number.

**FIGURE 13:**

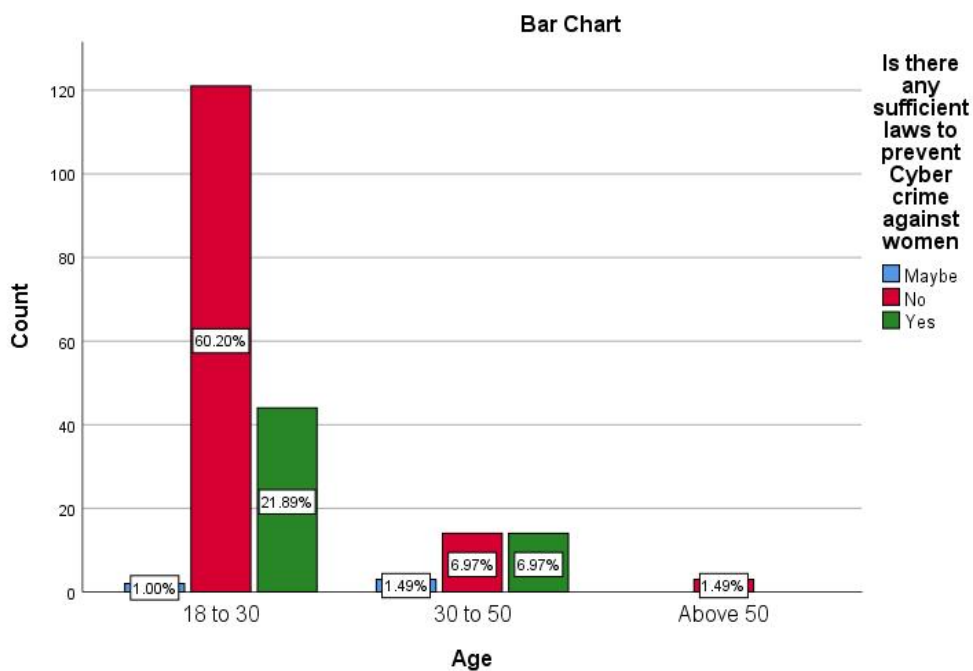
GENDER \* Whether women is considered as a soft targeting in cyber crime



**LEGEND:**

In the above barchart fig 13, we can see that the dependent variable whether women is considered as a soft targeting in cyber crime out of which male has responded YES in more number.

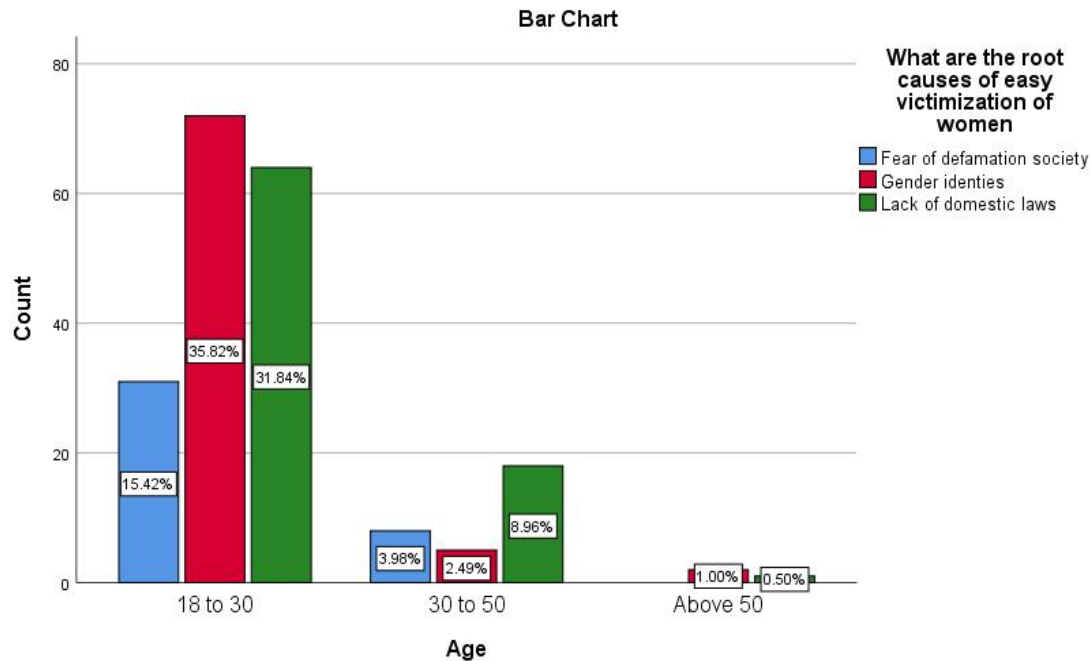
**FIGURE 14:** AGE \* Is there any sufficient laws to prevent cyber against women



**LEGEND:**

In the above barchart fig 14, we can see that the dependent variable is there any sufficient laws to prevent cyber crime against women in which age limit 18-30 have responded YES in more number.

**FIGURE 15: AGE \* What are the root causes of easy victimization of women**



**LEGEND:**

In the above barchart fig 15, we can see that the dependent variable what are the root causes of easy victimization of women in which age limit 18-30 have responded Gender identities in more number

**IV. RESULTS**

The independent pie chart analysis has been discussed from fig. (1 - 4) . Here, fig. 1 resulted that gender male answered more. Fig.2 resulted in age limit between 18 - 30 limit responded more. Fig.3 - education qualification where Undergraduate responded more. Fig.4 - Occupation analysis where students responded more. Fig.5 (5-9) dependent variable where fig5 resulted that many responded YES for cyber crime against women increased in present. In Fig.6 many responded NO for saying insufficient laws. Fig.7 many responded for the lack of domestic laws for root cause of easy victimization. Fig.8 many has responded YES for government had taken positive steps to avoid domestic violence. Fig.9 many have responded YES for Women in considered as soft targeting in cyber crime. From Fig. (10-13) SPSS comparative test done and compared with gender table and the analyses we got from it has been recorded that male responded more stating cyber crime against women still prevailing laws are insufficient and women are said to be soft targeting in cyber crime. Fig. (14-15) SPSS comparative test done and compared with gender table in the analysis we got it from was age limit of (18-30) insufficient laws to control cyber crime against women and gender identities is the root cause of easy victimization of women.

**V. DISCUSSION**

Fig.1 - In the above pie chart, we can see that the independent variable gender response have been analyzed in which male have been responded in more number. Fig.2 - In the above pie chart, we can see that the independent variable age response have been analyzed in which 18-30 have been responded in more numbers . Fig.3 - In the above pie chart, we can see that the independent variable educational qualification response is analyzed in which undergraduate has been responded in more number . Fig.4 - In the above pie chart, we can see that the independent variable educational qualification response is analyzed in which undergraduate has been responded in more number . Fig. 5 - In the above

pie chart, we can see that the dependent variable whether the cyber crime against women increased at present YES has been responded more. Fig.6 - In the above pie chart, we can see that the dependent variable Is there any sufficient laws to prevent cyber crime against women NO has been responded more Fig. 8 - In the above pie chart, we can see that the dependent variable whether government takes any positive steps to avoid domestic violence YES has been responded more. Fig.9 - In the above pie chart, we can see that the dependent variable whether women is considered as a soft targeting in cyber crime YES has been responded more. Fig. 10 - In the above bar chart, we can see that the dependent variable whether the cyber crime against women increased out of which male has responded more in number stated YES. Fig.11 - In the above barchart, we can see that the dependent variable Is there any sufficient laws to prevent cyber crime against women out of which male has responded YES in more number. Fig. 12 - In the above barchart, we can see that the dependent variable whether government takes any positive steps to avoid domestic violence out of which male has responded YES in more number. Fig.13 - In the above barchart, we can see that the dependent variable whether women is considered as a soft targeting in cyber crime out of which male has responded YES in more number. Fig. 14 - In the above barchart, we can see that the dependent variable is there any sufficient laws to prevent cyber crime against women in which age limit 18-30 have responded YES in more number. Fig. 15 - In the above barchart, we can see that the dependent variable what are the root causes of easy victimization of women in which age limit 18-30 have responded Gender identities in more number

## VI. SUGGESTIONS

To summarize, while a crime-free society is impossible to achieve and only exists in fantasy, it should be a continuing effort to enforce regulations that reduce criminality to a minimum. Particularly in an increasingly technologically reliant world, criminality related to electronic law-breaking is certain to increase, and legislators must go the extra mile to keep impostors at bay. Technology is often a double-edged sword that can be employed for either good or evil purposes. To combat cybercrime against women, the Legal system has enacted a number of legislation. Thus, it should be the relentless efforts of rulers and legislators to assure that technology advances in a healthier way and is employed for legal and ethical economic growth rather than criminal activity.

## VII. LIMITATIONS:

The major limitation of the study is the sample frame .The sample frame is collected through survey by giving the respondents the questionnaire, the real field experience is carried out. The survey was conducted in maduravoyal in Chennai ..The responses collected from are the people who are mostly educated and who are mostly from rural areas and if the responses are collected from people who are rural areas, the information on Cyber crime against women would be more accurate. This is the limitation of the study.

## VIII. CONCLUSION

In the cyber world women are subjected to harassment via email, morphing, cyber defamation, Social Networking, hacking, cyber-stalking, cyber pornography, cyber flirting and cyber bullying. Some awareness best practices and Tips can help women to be safe from these cyber-attacks and protect them and their families. As part of this project, Information Security Education and Awareness, we are trying to spread this awareness to women and help them to follow the best practices in using Internet, Smart phones and various other new cyber technologies through which attacks are most likely to happen. Beware of fake profiles. Maintain your privacy online, Check your account settings regularly, Don't let others peep into your accounts, Avoid participating with unknown members in chat rooms., Check the authenticity of the people who are praising you online. With increasing traffic in the virtual world, the chances of falling prey to cyber crime loom large all the while, more so in the case of women who are often seen as soft targets. The categories of online crimes targeting women have expanded and the wave has neither left India alone. A few more new generation crimes that are worth a mention here are cyber flames, cyber eve- teasing, and cyber flirting and cheating. Women in India by and large shy away from reporting matters, fearing potential negative media publicity, which may irreparably impact their reputations. The more time women spend online, without being completely aware of the pitfalls of the internet, the more vulnerable they become. Women should be more alert to protect themselves from targeted online attacks. From the study it is concluded that in India, the future of the Internet is still up for grabs

between cyber criminals and women Internet users. Fears of a cyber- apocalypse still abound. The Indian IT Act 2000 is not effectively enacted due to some deficiency and therefore, there is a increase in the rate of cybercrimes against women in India.

#### REFERENCES

- [1]. Introducing cyberspace. *Mapping Cyberspace* 2003; 13–43.
- [2]. Bichwa, Khatri R. Identify Cyber Bulling words using Clustering for Social Media. *International Journal of Computer Sciences and Engineering* 2018; 6: 525–528.
- [3]. Makori A, Agufana P. Cyber Bulling Among Learners in Higher Educational Institutions in Sub-Saharan Africa: Examining Challenges and Possible Mitigations. *Higher Education Studies* 2020; 10: 53.
- [4]. Kim J-Y. The Moderating Effect of Aggression in the Influence of Experiences of Violence in School on Cyber Bulling of Middle School Students. *Korean Association For Learner-Centered Curriculum And Instruction* 2020; 21: 1033–1046.
- [5]. Potharst ES, Schaeffer MA, Gunning C, et al. Implementing ‘Online Communities’ for pregnant women in times of COVID-19 for the promotion of maternal well-being and mother-to-infant bonding: a pretest-posttest study. *BMC Pregnancy Childbirth* 2022; 22: 415.
- [6]. Halder D, Jaishankar K. *Cyber Crimes against Women in India*. SAGE Publications India, 2016.
- [7]. Saxena S. *Crimes Against Women and Protective Laws*. Deep and Deep Publications, 1995.
- [8]. Gragido W, Pirc J. The Rise of the Subversive Multivector Threat. *Cybercrime and Espionage* 2011; 135–151.
- [9]. Bector P, Professor A, BPR College, et al. The Harmful Effects of Cyberbullying on Teenagers – Acommonstudy. *Global Journal For Research Analysis* 2012; 3: 1–3.
- [10]. Sheinov VP, Belarusian State University. Cyberbullying in youth environment: Origins and effects. *The Herzen University Studies: Psychology in Education*. Epub ahead of print 2019. DOI: 10.33910/herzenpsyconf-2019-2-73.
- [11]. PAKISTAN: Call to curb rise in violence against women. *Human Rights Documents Online*. DOI: 10.1163/2210-7975\_hrd-9943-2016039.
- [12]. Mansfield-Devine S. Significant rise in cybercrime against public sector organisations. *Computer Fraud & Security* 2012; 2012: 1–3.
- [13]. Choudhary R. Cyberspace and Women- Dimensions of Cybercrime against Women in India. *Design Engineering* 2022; 73–80.
- [14]. Rai K, Kaur B, Sardana S. Awareness of Cybercrime against Women among Students of Higher Educational Institutes in Delhi. *Performance Management* 2020; 163–174.
- [15]. Chang LYC. Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia. *The Palgrave Handbook of International Cybercrime and Cyberdeviance* 2020; 327–343.
- [16]. Bist AS. *CYBER CRIME AGAINST WOMEN IN INDIA –INVESTIGATIVE AND LEGISLATIVE CHALLENGES*. Blue Rose Publishers, 2020.
- [17]. Fatima T. *Cyber Law in India*. Kluwer Law International B.V., 2017.
- [18]. Bailey J, Flynn A, Henry N. *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Group Publishing, 2021.
- [19]. A. K-PDB, Mehdi. *Encyclopedia of Criminal Activities and the Deep Web*. IGI Global, 2020.
- [20]. Willems E. Cyberdangar. Epub ahead of print 2019. DOI: 10.1007/978-3-030-04531-9.