

# Are Women a Soft Target for Cyber Crime in India

Showkat Ahmad Dar<sup>1,\*</sup>, Dolly Nagrath<sup>2</sup>

<sup>1</sup>Department of Political science and Public Administration, Annamalai University, Tamil Nadu, India

<sup>2</sup>Department of Political science, Annamalai University, Tamil Nadu, India

Received: 01.06.2022 • Accepted: 26.06.2022 • Published: 30.06.2022 • Final Version: 30.06.2022

**Abstract:** A growing global issue that might have significant social and economic repercussions is cyber violence against women. This is due to the growing popularity of social media, the spread of information via mobile devices, and the growth of the internet. Any form of sexual or gender-based violence against women that takes place through ICTs like the Internet, mobile devices, and video games is referred to as cyber violence. These technologies are ideal for using as weapons against women for a variety of reasons these include cyber stalking, sexual abuse (including sending sexually explicit or pornographic emails to the victim), cyber extortion, cyber bullying, cybersex trafficking, and phishing. Even if there are more crimes against women overall, a woman can find that experiencing a cybercrime is the most upsetting thing that has ever happened to her. More so in India, where women are devalued and cybercrimes aren't even given significant legal consideration. India's legal system's current rules and practises are shown to have gaps in Cyber Crimes against Women, as well as what can be done to keep individuals secure online. In this essay, I'd want to discuss the various cybercrimes that can affect women and how they can harm them. I also briefly discuss new laws that are being introduced in this field, such as the Criminal Amendment Bill, as well as the many statutes that protect women in these circumstances, such as the Information Technology Act of 2000. (2013). to reach a conclusion, I consider a number of well-known cybercrime cases. Additionally, we need to consider a couple of answers for the rising frequency of cyber crimes against ladies in India. At the end, we talk about the choices accessible to casualties of cyber crime and the changes that should be made to the overall set of laws to battle the rising tide of cyber crimes.

**Keywords:** Cyber Crime, Women, Violations, Laws, Covid, and Challenges.

## 1. Introduction

Internet exists. Unthinkable things are now possible. Millions are adopting the internet due to machine reliance. Internet provides website, email, and IT solutions. Internet is a social boon, but it also enables criminality. Contact by e-mail and website. Internet is fast and worldwide. 2021 (Sharma) "Every nice side has a nasty side" Internet and computers are alike. Internet advancements undermine legislation. Internet crime is ineffective since it's unregulated and geographically irrelevant. Modern crime methods and media aren't covered by existing law. It's hard to identify, report, and verify India's cybercrime. Computer crime is unpoliced and unaudited. Cybercrime and electronic transactions as well as digital signatures astonish lawyers. Conventional laws have shown to be useless and dumb. Sharma will be in charge of the organisation in 2021. Weak evidence, but the pictures are the most important. As the internet matrix has changed the law, cybercriminals are adapting their approaches. There has recently been research into the gaps in cybercrime that offers a

\* Corresponding Author: darshowkat41@gmail.com

roadmap for the future. Group's proposals were approved by CCPWC. Under Section 77 of the Indian Penal Code, offenders are still subject to the Indian Penal Code's penalties, and the IT Act's penalty does not exonerate them of other offences. Many women have been victimised by internet stalking and cybersex as well as the sharing of obscene content.

Out of more than 600,000 cybercrime complaints, 12,776 first information reports were made in 2021. According to the research, total offences against women dropped from 12,902 to 9,782 in 2020. In 2020, 938 women were assaulted, down from 1,088 in 2019, and 862 were harassed, down from 644. In 2020, there were 967 rape incidents, a 21% decline from 2019. In 2020, there were 388 stalking reports, down to 235. In 2020, there were 35,331 crimes against women in the 19 largest cities, a decrease of 21.1 percent from the previous year (44,783 cases). "Cruelty by spouse or his family," "attacks on women with the goal to degrade her modesty," and "kidnapping and abduction of women" were the next most common crimes against women (7.2 percent). In 2020, there will be a 55 percent growth in the city's cybercrime, according to the data. Compared to 2019, 2020 has more than twice as many instances. Between 2019 and 2020, the number of people who posted sexually explicit behaviours and content climbed from 19 to 59. While the prevalence of cyber stalking increased from 16 to 12 that of cybercrime decreased from 11 to 31.

The number of incidences of online bank fraud rose from two in 2019 to 19 in 2020. There were 18,657 cybercrimes in urban areas, a 0.8 percent increase from 2019. (18,500) there was a 16.2% increase in cybercrime in 2020. In 2020, 11,356 cybercrimes, or 60.9% of all cybercrimes, targeted Section 66 of the IT Act. Fraudsters were inspired by COVID-19 to invent new con games, senior law enforcement official claims (NCRB Report). In 2021, there were 12,776 first-time reports of cybercrime out of more than 600,000 total reports.

## 2. Literature review

The first step is to identify any issues. It's essential that you read academic literature in order to become a better researcher. Cybercrime has an effect on artworks. There is a void, as this investigation indicates. 19 female cybercriminals were identified by Covid. Women may be more harmed by cybercrime than by other forms of violence, according to new research. In India, cybercrime is not given the attention it deserves. There has been a lot of discussion about women and cybercrime. Misra spoke about the CAB and the Information Technology Act of 2000, 2013). He did research on cybercrime (like Ritu Kohli). This article focuses on women's cybercrime.

Indian history advances: Violating women's rights is violent. Violence against women remains despite the efforts of feminists. IT empowered women and created a "Global Village." Women used the web, phones, and tablets Cybercriminals were aided by these tools, notwithstanding their advantages (Singh, J., 2015). Fraud attacks women more often than men. Criminals are hard to catch since there isn't enough evidence and people are afraid of being slandered. A few instances of the outcomes of cybercrime include libel, sexual harassment, and pornography. Emails and phone calls are made to women from unfamiliar email addresses that are disrespectful and frightening. As a result, they suffer and sometimes try suicide. Violent attacks on Indian women have been discussed online. Women's cybercrime was investigated in terms of its origins, manifestations, and response.

ICT has enabled ladies. Email is helpful. Women's activists condemn Internet wrongdoing against women and porn as prejudicial. Cybercriminals target kids dependent on WhatsApp, Facebook, Twitter, MSN, and MySpace (Poulpunitha, et.al. 2020). Digital reliance supports cyber crime. Absence of abilities and information causes cyber crime in India. Policing cyber crime-wise. India should utilize tech and regulation to battle cyber crime. Cybercrimes against women and girls need

technology, behaviour, law, education, and training. This study prevents cybercrime against women and girls.

Article says social media is ubiquitous. Information distribution, cybercrime. Lawlessness online causes cybercrime. Cyber stalking, pornography, and slander affect them. Cybercrime against Indian women is social and psychological (Chaudhary, V 2019). Slander hides most cybercrimes. Educate networkers. Parents, teachers, judges, police, and investigators could collaborate.

ICT enhances communication, idea sharing, and worldwide linkages. ICT is increasingly used against women (Kaushik, N. 2014). Avoid social media and the Internet. Texting, emailing, Facebook, Twitter, Craigslist, LinkedIn, and YouTube.

Networks are used in cybercrime. Indian cybercrime isn't out of the ordinary. Because to advances in technology, the Internet can now be abused and misused more easily. In 2016, India was third in the world for "malicious acts" after China and the United States. (Mallapur 2016). 512 million Internet users are expected in India by 2022. (2019) in the digital age, there has been an upsurge in online crimes such as phishing and spyware. An in-depth look at India's legal system was provided in the book. (Rameesh .S 2020).

### **3. Statement of problem**

Society, government, families, and people must respond quickly to cybercrime. Few reliable crime statistics are available, and most offences go unreported. Specific and effective study on cybercrime prevalence and prevention is needed. Internet use has skyrocketed in 20 years. Later, scholars studied similar problems. This study analyses methods to safeguard and prevent cybercrimes against women and girls.

### **4. Research objectives**

1. To know more about how women are targeted by cybercrime.
2. To determine the best ways to protect women from being victims of cyber crime.
3. To reveal an insight into lawful arrangements about cybercrime against Women.

### **5. Methodology**

Doctrinal or non-empirical research methods were utilized to compose this article. To survey current resolution arrangements and case regulation, this article will utilize thinking and investigation. Utilizing essential and auxiliary sources, including regulation, case regulation, lawful course readings, critiques, books and sites on the web, news stories, and other unfamiliar distributions and magazines, among others, this paper tried to approve all assumptions. Analytical research and ex post facto (done, made, or figured out sometime later) are both applicable to the ebb and flow Study.

### **6. Discussion and result**

Cyberspace, the online environment created by computers, is governed by cyber laws. All users worldwide are subject to these limitations. Networked IT is covered under cyber legislation. Worldwide testing for pandemic. People had to deal with poor access to healthcare, suffering and loneliness during lockdowns, losing their jobs, and losing loved ones. Globally, the COVID-19 outbreak has claimed millions of lives. The epidemic has claimed millions of lives and put millions of people through misery, including those who lost their jobs or had to shut down their

companies because of lockdowns, families who lost their sole breadwinner, young children who lost both parents, and others. Incorrect! Cybercrime and mobile crime both spread quickly during the outbreak. Some people tortured others during the pandemic by using the internet and mobile devices. The epidemic increased cybercrime.

### **Cybercrime**

The 2000 IT Act of India makes no mention of cybercrime. Crimes and penalties are outlined in the 1860 Indian Penal Code and other statutes. Technology and crime are combined in cybercrime. Computer offences are a part of cybercrime. Cybercrime is the term for online crimes when the perpetrator isn't required to make eye contact with someone or reveal his or her identity. Computers or data are used as a target or tool in cybercrime. The crimes listed above fall under cybercrime.

The law is undermined by the internet and other technology. The open, unregulated, and geographically irrelevant nature of internet crime makes it ineffective. Existing criminal law does not apply to contemporary criminal tactics and media. In India, it is challenging to recognise, report, and prove cybercrime. Computer crime requires computer experts and is not audited or policed. Lawyers are astounded by electronic transactions, digital signatures, online transactions, and cybercrimes. Traditional laws are useless in today's streamlined, less criminalised world. The case is tenuous. Visual evidence is essential. The legal system has been shaken up by the internet, and new tactics are being used by cybercriminals.

The IT Act of 2000 (Kumar, A., and Ranjan, A. P. (2022) doesn't shield ladies' humility, regardless of the way that the Indian constitution awards them equivalent freedoms to life, instruction, well being, food, and work. In contrast to the Indian Penal Code, the Constitution, or the CCP, the IT Act, 2000 doesn't address wrongdoing against ladies. A specialist board was as of late collected by the public authority to assess cyber-crime holes and proposition a guide. In light of the proposals of the gathering, the public authority took on CCPWC. As per Section 77 of the IT Act, the Indian Penal Code keeps on applying in all circumstances and that the IT Act's discipline doesn't excuse the guilty party from different regulations. Cyber stalking, digital slander, cybersex, the transmission of explicit material, and protection encroachment are fairly pervasive.

### **Victims of cybercrime**

During the outbreak, women were the most vulnerable, making them easy targets for hackers. During the pandemic, social media users and stay-at-home moms were singled out for attack. During a lockdown, cybercrime against women increases, but later decreases, according to the National Commission on Women in 2021. By April and May 2021, as a result of the second Covid-19 wave of attacks, cybercrime against women had skyrocketed. As the second pandemic wave subsided and lockdown restrictions were loosened, cyber-attacks began to diminish in June and continued to decline in July. Cybercrime against women was rare prior to the outbreak and closure.

### **Cybercrimes against women**

It was common for individuals to utilize the internet for everything from school and business to pleasure and socializing throughout the pandemic and lock down. Women can now work from home thanks to laptops, smart phones, and the internet. Participation in online learning and other activities is mandatory for female students. As more women turned to social media and the internet for their professional and academic pursuits, as well as for personal enjoyment, cyber crime rose. This

resulted in an emotional and mental attack on the victim as a result of being locked out. Among the most common cyber crimes affecting women are:

There are several forms of cyber stalking, which includes posting (often threatening) remarks on someone else's Facebook page and making phone calls or texts to the victim despite their lack of interest. In the year 2021, the B. D. Sharma scholar group published the book According to a survey, 62.5 percent of online harassment stemmed via emails and chats. Ritu Kohl's story sparked the creation of new regulations to safeguard crime victims. Up to three years in prison and a fine are available under ITAA 2008 Section 66A for anyone found guilty of disseminating obscene material using electronic communication services, among other means.

It is common knowledge that during the epidemic, most of the people who commit this type of crime are women. For sexual favours or money, thieves blackmail their victims into handing over private photos or images that have been tampered with. The pandemic-frustrated criminals utilised the approach of threatening women for sex in letters or video conferences. Despite the fact that they had no means of support, they could nevertheless threaten others by posting fake photographs online.

Cyber hacking during the pandemic era made headlines on the internet. False news and misinformation are becoming increasingly common. Their personal data was acquired, the microphone and camera were activated on and intimate photographs and videos were taken by malware URLs that they clicked on. Criminals exploit the information and photographs to commit sexing and other offences.

Derogatory remarks on the victim's page and asking money to get them removed are two examples of cyber bullying. Also, private or changed images of the victim without her knowledge are traded without her permission (Singh, J. 2015). It is possible to perform online harassment and abuse using computers, cell phones and laptops.

Notwithstanding digital phishing, there are various alternate ways of abusing PCs, telephones, and PCs. Clicking a connection in a phishing email fools the casualty into uncovering individual data such their financial balance number, contact subtleties, and passwords, and the casualty's gadget is then tainted with dangerous infections. In the expressions of (Jagdish Singh 2015). The hoodlums use the casualty's ledger and other individual data to commit misrepresentation.

Predators have involved photos of individuals for porn on the web. Public morals led to the deactivation of 857 pornographic websites in 2015. Ravi Shankar Prasad was the one who lifted the embargo. Because sexuality is a personal choice, the state should not impose its morality on others. There is no restriction of pornographic websites or foreign ISPs. According to Singh, the law prohibits child pornography, but it doesn't specify what constitutes child pornography (2015). Domestic pornography should be allowed. Save it to your computer, mobile device, or other storage medium of your choosing.

Under the IT Act, pornography on the Internet is completely unrestricted. According to Indian courts, internet pornography must be a component of "public order." They refer to this as "legal maintenance" in their paper by the same name by Kumar, A. and Ranjan, A. Sections 66A.E, 67, 67A, and 67B provide information on cyber pornography. Except for sections 67A and 67B, the Information Technology Act of 2000's Section 77B allows for pornographic bail.

Cyber trafficking victims never encounter their abusers in person. In the practise of cybersex trafficking, the victim's sexual or intimate behaviour is publicly broadcast, recorded, or photographed and then sold online. Women were coerced and threatened by cybercriminals.

### **Legal provisions**

Despite the lack of a formal regulatory framework, many statutes can protect cyber assault victims. Penal Code of 1860 before 2013, it was not against the law to harass or abuse women online. Amendments to the Indian Penal Code were made under Section 354A of the Criminal Amendment Act of 2013. The punishment for a man who solicits or requests a woman's sexual services, displays pornography without her consent, or makes sexual remarks is up to three years in prison or a \$2,500 fine, or a combination of the two a fine or a jail sentence in the first two situations. It is illegal to engage in voyeurism without the agreement of the woman. The lady must "expect not to be watched by the offender or anybody acting at the perpetrator's direction" for voyeurism. First-time offenders are sentenced to three years in jail, while repeat offenders are sentenced to seven years in prison. Cyber stalking is outlawed in 354D, which prohibits the practise. In the case of stalking, a man pursues or monitors a woman's online behaviour despite her indifference. Three years in prison and a fine for first-time stalkers; five years for repeat offenders. In addition to amendments to the Code, other laws can be used to punish cyber offenders. Include:

Slander is defined in Section 499 as the act of defaming another person's character or reputation. Defamation is punishable by up to two years in prison, a fine, or both, if a defamatory statement is published.

When someone's reputation is threatened, Section 503 bans it (Sharma, B. D. 2021). As demonstrated, cyber extortion is covered by this statute.

Maximum penalty for (Sharma, B. D. 2021) Criminal Intimidation by an unknown perpetrator is outlined in Section 503. Section 503 offences, such as criminal intimidation, are punishable under this section.

If a person utters, produces, or presents an object or sound that degrades or invades the private space of a female, they can be sentenced to up to three years in prison and a fine. Sexually explicit comments, images, and other content may be punished by this clause.

### **2000's Information Technology Act**

Section 66C of the IT Act expresses that wholesale fraud is a wrongdoing rebuffed by regulation. Hacking is the subject of this condition. This regulation considers as long as three years in jail and a fine of Rs. one lakh for the deceitful utilization of someone else's electronic mark, secret key, or other novel recognizing characteristic.

Section 66E of the Privacy Act oversees infringement of security. Catching a picture of somebody's confidential region without their consent is deserving of as long as three years in jail as well as a fine, contingent upon the seriousness of the wrongdoing.

Profane substance is unlawful under Section 67, which rebuffs violators with as long as three years in jail and a fine for the main offense and as long as five years for the second.

The Civil Code's Section 67A an offense deserving of as long as seven years in prison and charge for the scattering of physically unequivocal substance comprises a misdeed deserving of as long as five years in jail and fine for the primary offense.

### **Indecent Representation of Women Bill 2012**

The measure prohibits the publication, advertising, and other forms of media from depicting women in an indecent or otherwise offensive manner. Proposal: Law should be amended to include

audiovisual mediums, electronic materials, Web distribution, and depictions of women on the Internet (Sharma, B. D. 2021). When the statute expired in 2021, it was repealed.

### **Some Suggestions and Steps to Tackle Cyber Crimes**

Self-cyber victimisation is dangerous, and women need to be aware of this and speak out against it. Different nations have different cyber laws. Women today want to browse the internet discreetly and securely. Dealing with this is necessary. By using the following advice, women can maintain the security of their online interactions:

We recommend passwords that are simple to remember. Passwords on all online accounts should be changed on a frequent basis to protect privacy and security (Pennell 2012). Phones, email, landlines, banking, and credit cards are all secured by difficult-to-crack passwords. Do not divulge your secrets too soon (Moore, 2009). You can make secure passwords using any combination of letters, numbers, and symbols. Avoid using dictionary phrases, dates, or special website passwords as passwords (Online Privacy & Safety Tips 2010). Passwords are used to protect privacy.

If you're a well-known businesswoman, be careful about giving out your home location. Either a job or a mailbox will do. To protect yourself from cyber predators (Moore 2009). Women should refrain from posting private information online.

A minimum of 2000 supporters would be ideal. 150 people can be friends, according to Dunban7. We probably only know 150 of the 2000 Facebook users. We must restrict access to our information in order to guarantee that only people we know have access to it. (J. Singh (2015). Avoid unreliable friends.

In both schools and colleges, there needs to be a greater emphasis on raising awareness of issues like stalking, financial dishonesty, libellous behaviour, improper use of email and social networking sites, virtual rape, cyber pornography, email spoofing, etc (Halder and Jaishankar 2010). There are currently anti-cybercrime programmes in effect.

Law enforcement, social care providers, and nonprofits organisations should all be involved in an inquiry into adult internet usage. Law enforcement and non-profit organisations must be notified about cybercrime, according to Singh (2015). Second, police officers must attend specialised training sessions and seminars to help them understand victimisation accusations. Everyone, including academics, attorneys, and non-profits, must attend workshops and seminars (Halder and Jaishankar 2010: 22).

In India, women must be safeguarded from online crime. A separate cybercrime law or the IT Act of India must be updated to combat cybercrime (Halder and Jaishankar 2010: 22). By upholding the law, society can be improved.

Unwanted calls and SMS messages may be monitored. If the harasser calls again, you should contact the police (Halder and Jaishankar 2010: 21). Make sure the software you purchase comes from a reliable source. They should let their parents, partners, or spouses know what they are doing online. By altering the privacy settings, you may manage how online services handle your personal information. Any applicable privacy policies should be understood and followed. Recognize the privacy settings for social media (Pennelli 2012).

Fight According to Singh, J., email infestations, worms, and Trojans are tools frequently used by cyber stalkers (2015). Anti-virus software needs to be updated frequently in order to prevent against Trojan, email, or worm infestations (Pennelli 2012). Cyber bullying can be prevented.

Watch out for any unusual behaviour on your network account at all times. Examine email, blogs, and WebPages for any unusual behaviour. By keeping an eye on our accounts, we can avoid being hacked or followed. Some ladies simply don't bother when it comes to online activities. He became stuck when a check was made (Moore 2009). This cannot be disregarded.

We routinely use the computers in internet cafes. Public computer browsers keep track of passwords and websites visited. Clear the cache and history on your browser before moving on (Doyle 2012). Indifference can have disastrous results. Avoid online stalkers at all costs. The firewalls, which are intended to prevent hackers and unknown websites out, are unable to access phoney or unknown websites. On a select few operating systems, firewalls made for a single computer come preinstalled.

The system is protected against an attacker when the computer is turned off. Cybercrime's damage can be lessened by limiting it (Cybercrimes Report 2012: 3-4). Cybercrime should worry both men and women. When it comes to the Internet, mobile devices, and cyberspace, there are two sides to every coin. There are numerous tools at users' disposal to keep them safe online. The funding for cybercrime research should come from the Indian government. The criminal justice system benefits from education.

## **7. Conclusion**

We can't eliminate crime, but we can make our neighbourhoods safer. In a technology-dependent society, policymakers and law enforcement must deter online lawbreakers. Technology is beneficial and bad. Several laws concern cybercrime against women. Government and lawmakers must ensure technological innovation is lawful and ethical. As more people utilise the internet, especially vulnerable women, criminal activity escalates. India's online crime reports against women are rising. Teens cheat, flirt, and set virtual fires. Indian women worrying about unfavourable media are reasonable.

Spending more time online without knowing the consequences puts women at risk. Never harass women online. Cyber law grows along with cybercrime. Cyber law must handle these online threats. As quickly as possible, governments and cyber law organisations should be notified. India funded internet trend research in 2013 and 2014. In 2014, India held a cyber law conference. These programmes boosted intellectual and international cooperation. Despite having few cyber courts, India's police force is well-trained. Online crime hasn't decreased.

### **Announcement of ompeting Interest**

The creators state unequivocally that they have no known contending monetary interests or individual associations with outsiders that would have given the presence of affecting the work uncovered in this review.

### **Acknowledgement**

The creators need to offer their most profound thanks to analysts who stayed mysterious for the quick remarks and suggestions they gave to assist with working on the general nature of this paper.



## References

- [1] Ahmed, D. F. (1992). Cyber Law in India (Laws on Internet).
- [2] Chaudhary, V. 2019 "Cyber Crime against Women" international educational journal chetna volume 1
- [3] Datta, P., Panda, S. N., Tanwar, S., & Kaushal, R. K. (2020, March). A technical review report on cybercrimes in India. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 269-275). IEEE.
- [4] Dhupdale, V. Y. (2014). Cyber Crime and Challenges Ahead. Handbook of Cyber Laws, 1.
- [5] Gordon, F., McGovern, A., Thompson, C., & Wood, M. A. (2022). Beyond cybercrime: New perspectives on crime, harm and digital technologies. *International Journal for Crime, Justice and Social Democracy*, 11(1).
- [6] Graham, A., Kulig, T. C., & Cullen, F. T. (2019). Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. *Policing: An International Journal*.
- [7] Hussein, O. A. (2022). Cyber Blackmail Crime against Women-A Case Study. *Journal of Positive School Psychology*, 6(3), 6882-6893.
- [8] Jain, M. J., & Chaudhary, M. R. (2019). Understanding the concept of cybercrimes in India Vis-a-Vis cyber laws of USA. *IJRAR-International Journal of Research and Analytical Reviews (IJRAR)*, 6(2), 427-438.
- [9] Kaushik, N. (2014). Cyber Crimes against women. *Global Journal of Research in Management*, 4(1), 37
- [10] Kaushik, N. (2014). Cyber Crimes against women. *Global Journal of Research in Management*, 4(1), 37.
- [11] Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, 37(4), 480-501.
- [12] Kethineni, S. (2020). Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. *The Palgrave Handbook of International Cybercrime and Cyber deviance*, 305-326.
- [13] Kethineni, S. (2020). Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. *The Palgrave Handbook of International Cybercrime and Cyber deviance*, 305-326.
- [14] Kumar, A., & Ranjan, A. P. (2022) Prevailing Cyber Security Law. *Supremo Amicus Journal PIF 6.242*
- [15] Lumsden, K., & Harmer, E. (2019). Online othering. *Palgrave Studies in Cybercrime and Cyber security*.
- [16] Misra, R. (2013). Cyber Crime against Women. Available at SSRN 2486125.
- [17] Pallathadka, H., Kumar, S., & Kirana, L. P. (2021). Cyber-crime against children and women: A study with specific reference to covid-19 pandemic times. *Journal of Cardiovascular Disease Research*, 245-257.
- [18] Poulpunitha, S., Manimekalai, K., & Veeramani, P. (2020). Strategies to prevent and control of cybercrime against women and girls. *Mental*, 81, 81-0.
- [19] Poulpunitha, S., Manimekalai, K., & Veeramani, P. (2020). Strategies to prevent and control of cybercrime against women and girls. *Mental*, 81, 81-0.
- [20] PTI. (2015, August 3). 857 porn sites banned in India; Govt plans ombudsman for Net content. *Www.Financialexpress.Com*. <https://www.financialexpress.com/industry/technology/porn-ban-in-india-sparks-censorship-debateretrieved on 19 April 2022>.
- [21] Ravindran, S., & Shah, M. (2020). Covid-19: 'Shadow pandemic' and violence against women. Ideas for India. <https://www. Ideas for India. In/topics/social-identity/covid-19-shadow-pandemic-and-violence-against-women. Html>.
- [22] Sankhwar, S., & Chaturvedi, A. (2018). Woman harassment in digital space in India. *International Journal of Pure and Applied Mathematics*, 118(20), 595-607.
- [23] Sharma, B. D. (2021, April 21). Cyber Crime In India: Are Women A Soft Target. *Www.Legalserviceindia.Com*. <https://www.legalserviceindia.com/legal/article-639-cyber-crime-in-india-are-women-a-soft-target retrieved on 13 April 2022>.
- [24] Singh, J. (2015). Violence against women in cyber world: a special reference to India. *International Journal of Advanced Research in Management and Social Sciences*, 4(1), 60-76.