Educational Administration: Theory and Practice
2024, 30(2), 2195-2202
ISSN: 2148-2403
https://kuey.net/ **Research Article**

Cybercrime Against Women In India: Challenges, Legal Safeguards, And Preventive Strategies

Ms. Geeny Mourya[1*], Dr. Haidar Ali[2]

[1*]Research Scholar, Institute of Legal Studies and Research, Mangalayatan University, Aligarh, U.P., Email: bittu988@gmail.com
[2]Associate Professor, Institute of Legal Studies and Research, Mangalayatan University, Aligarh, U.P.

Citation: Ms. Geeny Mourya, et.al (2024). Cybercrime Against Women In India: Challenges, Legal Safeguards, And Preventive Strategies, *Educational Administration: Theory and Practice*, 30(2) 2195-2202
Doi: 10.53555/kuey.v30i2.11227

ARTICLE INFO

ABSTRACT

Crime against women is a prevalent issue in our society since practically every woman experiences abuse on a daily basis at some time in her life. Cybercrime in the contemporary world is scarcely a novel form of criminal activity. Any illegal activity conducted on or via computers, the Internet, or other technologies approved by the Information Technology Act is referred to as cybercrime. Criminals with technical expertise utilize the internet to carry out a variety of crimes. Cybercrime, taken more broadly, is any illegal activity that involves the use of a computer or the internet as a tool, a target, or both. The misuse of the increasing technological dependence of modern civilization gives rise to cybercrime, an uncontrollable evil. The necessity to promote user comfort has arisen from the rapidly growing use of computers and related technology in daily life. To deter and punish infractions of these rules, the Indian government focuses a great priority on teaching its people about women's rights. It's also critical that other participants in the criminal justice system, such as police enforcement, detectives, public prosecutors, and judges, learn about the laws regarding cybercrime against women and develop a deeper comprehension of these offenses. Furthermore, it is imperative to revitalize and increase the popularity of grievance redressal procedures and organizations. The main objectives of this effort are to streamline the complaint filing process and shorten the duration between investigations and prosecutions.

Keywords: *Cyber-crime, Society, Criminals, Online Scams, Women, Crime against women*

Introduction

The widespread use of internet technologies has unfortunately led to a significant rise in cybercrime, which affects women more than men (Singh & Gautam, 2022)**.** Traditional crimes have evolved to blend in with the online world, making it harder for police to do their jobs. This is why it is important to find out whether current policing systems are capable of handling these emerging digital threats. According to reports, one of the top four economic crimes that all organizations believe to exist is cybercrime (PwC, 2011). An ASSOCHAM research states that there would be an increase in cybercrimes worldwide as people look for unlawful ways to make money. The results of the surveys demonstrate how cybercrime has been rising globally at a startling rate. Cybercrime: What is it? “Any criminal act dealing with computers and networks (called hacking)” is the definition of cybercrime according to Webopedia (Vangie Beal, 2015). Cybercrime encompasses a variety of illicit digital actions directed at organizations to cause harm. In India, (KPMG, 2014) "Cybercrime is simply a crime that has some kind of computer or cyber aspect to it," is the most basic definition provided by Norton Company (Norton, 2015). As per Norton, cybercrime results in the theft of someone’s identity every three seconds. Boundaries and territorial barriers are irrelevant to cybercrimes. Ensuring the safety of the digital realm is a top priority for all parties involved.
Cybercrime, in its generalization, refers to the criminal actions performed by digital means, which poses a substantial threat to individuals and organizations, and women are often affected disproportionately (PARAMESWARARAO et al., 2021). To combat cybercrimes, each nation has established an Internet legislation or cyber law that governs the internet things of a country. The Indian government has also enacted a similar law entitled the Information Technology Act, 2000. The Act's original framework did not

include any specific provisions for gender-based cybercrimes, which has made it much less effective at prosecuting a wide range of offences, including cyberstalking, revenge porn, and other forms of online gender-based violence (Balabantaray et al., 2023). This legislative failure is explained by the fact that the Act is centered on facilitating the digital transactions, as opposed to the dynamics of cyber-harassment and abuse that are complex to consider, and thus demanded changes (Deo and Singh, 2022).Therefore, the changes were required to mitigate this issue and guarantee that women are properly safeguarded on the Internet (Singh and Gautam, 2022). Later amendments to the Information Technology Act in 2008 to expand the scope of the Act to various cyber offences highlight the development of a more profound understanding of the need to further develop the legal response to cybercrime (Borah, 2020; Deo & Singh, 2022).

12,776 initial information reports about cybercrime were made in 2021, out of over 600,000 complaints. The study shows that in 2020, there were 9,782 total offenses against women, down from 12,902 in the previous year. In 2020, there were 938 fewer assaults and 862 fewer harassments of women than there were in 2019 (1,088 versus 644). There were 967 rape cases in 2020 compared to 2019 a 21% decrease. There were 235 reports of stalking in 2020 compared to 388 in 2019. The 19 biggest cities saw 35,331 crimes against women in 2020, a 21.1 percent drop from 44,783 instances the year before. The third most common crimes against women, accounting for 7.2% of cases, were "cruelty by a spouse or his family," "attacks on women to degrade her modesty," and "kidnapping and abduction of women." The study indicates that cybercrime in the city would increase by 55% in 2020. 2020 has more than twice as many incidents as 2019. The percentage of individuals who shared sexually explicit actions and content on social media increased from 19 to 59 between 2019 and 2020. Cybercrime fell from 11 to 31, but the frequency of cyberstalking climbed from 16 to 12.

Online bank fraud incidents increased from two in 2019 to 19 in 2020. In metropolitan regions, there were 18,657 cybercrimes, up 0.8 percent from the previous year. In 2020, cybercrime increased by 16.2% to 18,500. Section 66 of the IT Act was the target of 11,356 cybercrimes in 2020, accounting for 60.9% of all cybercrimes. According to a top law enforcement official, fraudsters were inspired by COVID-19 to create other con games (NCRB Report). In 2021, there were 12,776 reports of cybercrime out of a total of over 600,000 complaints. Cyber victimisation often affects and targeted to women, and when there is no legal protection, online abuse turns into social harassment (Barak, 2005).

In the online world, a thorough legislative structure is mandated to protect women against cybercrime. As a result, the Indian legal system is required to significantly alter the current cyber laws, rules, and regulations. It is crucial to carry out a comprehensive analysis of the such activities in India that gave rise in cybercrimes specially targeting at women.

Cybercrime

Cybercrimes occur within the cyberspace, which encompasses computer networks and may occur in numerous situations in the real life. Such offenses include hacking security or destroying computer systems, including networks, websites, or computer programs. The scope of cybercrime is immense; however, it includes, but is not limited to, financial fraud and distribution of illegal information, as well as any other form of crime that uses computers or networks as a means or as a place (PARAMESWARARAO et al., 2021). Women-specific cybercrime focuses exclusively on women and uses digital mediums as the means of enacting these crimes, including cyberstalking, harassment online, sexual abuse by images, non-consensual sharing of intimate images, and more often has severe psychological and social consequences (Deo & Singh, 2022).

The overlapping of digital and physical spaces and the possibility of cyber violence perpetuated by real violence make this problem even more problematic, as cyber violence against women and girls can contribute to real-life violence, which is much more problematic through long-standing socioeconomic inequality (Panda, 2023). This is a critical approach that is consistent with feminist criminology, which states that online behaviours are simply the activation of offline social processes and interaction, which necessitates the reconsideration of the definition and treatment of gender aspects of crime in the conventional criminology (Lazarus, 2019). It might encompass fraud and solicited posts. It may entail foreign firms exploiting their trade secrets or government information without authorization across huge global networks. China has the most developed cyber defensive and is ahead of the United States, Canada, the Netherlands, and France (Sarmah et al., 2017; Chudasama, 2022).

Types of Cybercrimes

Categories of cybercrime affecting women in the majority of cases include cyber-harassment, cyber-stalking, revenge pornography and factoring in deep fake pornography (Lazarus, 2019) (Gius, 2023). Such forms often involve the unauthorized sharing of personal data, provocative images or malicious data, and use digital platforms to implement them (Gius, 2023). The numerous forms of cybercrime against women include all of these malicious actions: bot-networks, cross-site scripting, cyberbullying, cyberflirting, cyberhacking, cybermorphing, cyberstalking, cybersquatting, email spoofing, hacking, revenge porn, and phishing (Balabantaray et al., 2023). The prevalence of such activities indicates the influence of online behaviors on the reproductive and intensifying gender bias in the society and thus the need to examine and study online victims in further detail considering digital crimes. In fact, the issues of gender in the digital realm are often preconditioned by the problems they have in the society, therefore shaping the character, the logic, and the outcomes of victimization (Lazarus, 2019). The main challenge towards successful policing and prosecution

of these crimes is the fact that there is no standardized and universal system of classifying cybercrimes leading to the existence of different laws and practices in different jurisdictions. The identification of the nuanced differences between traditional cybercrimes and the particular ones specifically targeting women requires the introduction of the theoretic paradigm that incorporates feminist criminological approaches that would explain the gendered aspects of digital victimization into a coherent whole (Lazarus, 2019).

Provisions for Cybercrime Against Women in India

This table highlights the types of crime, the provisions and punishment for such crimes that highlights the contemporary legal framework to effectively combat the multifaceted challenges posed by cybercrime against women in India.

	Type of Crime	Provision under laws	Punishment
1.	Cyberstalking	Section 78, BNS (prev. Sec 354D IPC)	Up to 3 years (1st offence), up to 5 years (repeat offence)
2.	Cyber Bullying / Stalking / Sexting	Section 74 & 75, BNS (prev. Sec 354D/354A IPC); IT Act Sections 66A *(struck down)*, 67, 67A	Up to 3–5 years and fine depending on severity
3.	Online Harassment/Threats	Section 140, BNS (prev. Sec 506 IPC) IPC Section 507 (Anonymous threats)	Up to 2 years and/or fine
4.	Cyber Pornography (incl. morphing)	Sections 67, 67A, 67B, IT Act; Sec 176 BNS	3 to 5 years and fine
5.	Voyeurism	Section 77, BNS (prev. Sec 354C IPC)	1 to 3 years (1st), 3 to 7 years (repeat)
6.	Cyber Defamation	Sections 354, 356, 357, BNS	Up to 2 years and/or fine
7.	Doxxing (sharing personal info)	Section 66E, IT Act	Up to 3 years or ₹2 lakh fine, or both
8.	Sending obscene material	Section 67, IT Act; Sec 176, BNS	Up to 3 years and fine
9.	Email/Social Media Hacking	Section 66, IT Act	Up to 3 years or ₹5 lakh fine, or both
10.	Mail Phishing	Section 66C & 66D, IT Act	Identity theft & cheating by impersonation; Up to 3 years and ₹1 lakh fine
11.	Impersonation/Fake Profiles	Section 66D, IT Act	Up to 3 years and ₹1 lakh fine
12.	Cyberbullying	IT Act + Sec 74/140, BNS	2 to 5 years (varies by severity)
13.	Blackmail with intimate content	Section 67A, IT Act; Sec 73, 74, BNS	Up to 7 years
14.	Sextortion	Section 75, BNS	3 to 5 years depending on nature of offence

Cybercrimes are classified into the following:

1. Crime Against Individuals:

- **Cyberstalking:** Diversing or threatening a person on the internet.
- **Hacking:** Unauthorized entry into the computer systems or networks.
- **Identity theft**: stealing personal data of someone in order to impersonate them.
- **SMS Spoofing:** This is the use of fraudulent SMS messages to trick users.
- **Cyber Obscenity:** The dissemination or creation of obscene material on the Web.

2. Crime Against Economy: □

- **Computer fraud:** Fraudulent activities of computer or network.
- **Computer forgery and counterfeiting:** Faking documents or currency through the use of computer.
- **Computer sabotage:** The deliberate destruction of computer systems.
- **Cracking:** The act of cracking into a software or systems with the aim of obtaining unauthorized access.
- **Cybersquatting:** Registering the domain names with a view of making profits out of a trademark.
- **Economic espionage:** The theft of trade secrets or business secrets.
- **Intellectual property right infringement:** Infringement of copyright, patents or trademarks.
- **Malicious programs** (e.g., viruses, worms, Trojan horses, hoaxes): The production and dissemination of malicious (malicorous) software.

3. Crime Against Society:

- **Phreaking:** Using phone systems or networks.

- **Salami attacks:** The stealing of small sums of money on multiple accounts.
- **Tax evasion**: The unlawful evasion of taxes.
- **Telecommunication services theft:** Unauthorized telecom services.
- **Web jacking:** A seizure of a web site or a web server.
- **Cyber pornography:** The marketing or production of pornographic material on the internet.
- **Child pornography:** Production, giving, or being in possession of explicit material of children.
- **Racial and other hate speeches on blogs and social networking sites:** Distributing hate speech on the internet.

4. Crime Against Nation: □

- **Cyber terrorism:** The application of technology to cause fear or damage because of political or ideological motives.
- **Cyberwarfare:** State-funded assaults on the computer systems of other states.
- **Destruction of vital infrastructure:** Attacking important infrastructures such as power systems or transport.

Women and Cybercrime

Nowadays, cybercrime against women is a well-known problem. The new battleground where women's security, privacy, and dignity are being jeopardized every second is the internet. Every two seconds, one lady in India becomes a victim of cybercrimes. Some criminals use technology to target women for defamation. They send them obscene emails and WhatsApp messages, stalk them through websites and chat rooms, and worst of all, they use it to create pornographic videos, most of which are made without the consent of the victims. They also use it to spoof emails and manipulate images for pornographic content by using various online software programs (Kumar and Priyanka, 2019). Due to a lack of knowledge about where to report cybercrimes or an unwillingness to deal with the resulting social shame, Indian women are unable to report them promptly. Although regulations protecting women's security place more emphasis on physical harm than emotional harm, cybercrimes against women have more psychological impacts than physical ones. This suggests that women in particular need to have a more open-minded perspective and take the lead in reining in lawbreakers by going after them and filing complaints right away. If women report crimes promptly and alert the abuser, most of the issues may be resolved (Dhruti, 2019).

The Reasons Behind India's Cybercrime Against Women

Some of the reasons why cyber violence against women continues to increase every day in India are:

- **Digital Unawareness in Women:** Most women are not well versed with the concepts of online safety, privacy settings, and the ability to recognize the presence of suspicious activities, which makes them susceptible to cyber threats. Such digital illiteracy makes it more likely to be a victim of phishing, stalkers, Internet fraud, and identity theft.
- **Growing the digital presence:** The high score in cyberattacks in India, when compared to other countries in the world, proves that such threats are rampant and puts more women at risk of exploitation.
- **Reporting:** The reluctance of victims to report incidences is a major reporting gap that is usually caused by fear of social stigma, re-victimization or the lack of trust in the efficacy of legal recourse.
- **Personal feuds:** Such conflicts may culminate into online harassment, doxing, or even loss of reputation, particularly when personal data of a sensitive nature is at stake, which causes severe emotional and psychological trauma to the affected persons.
- **Financial gain:** Women are often targeted by cybercriminals to engage in financial exploitation by using phishing, online fraud, and sextortion, as well as employing social engineering strategies to get access to funds or sensitive personal information illegally.
- **Excessive use of Technology and Casual Internet use:** The widespread availability of digital technologies (including smartphones, social media platforms, and low-cost internet services) greatly contributes to the execution of cybercrime. The ease with which digital tools could be used is also an additional motivation as to why perpetrators will want to target women in the online space.
- **Gender Inequality and Patriarchal Mentality:** This is ingrained within the virtual sphere of the Internet, as women who voice their opinion or those who are active on social media are disproportionately harassed. The most common types of misogynistic behavior, abuse online, trolling, and threats are aimed at women because of their gender.
- **Ineffective Cybersecurity Habits:** Such common habits as the use of weak passwords, disclosure of a log in, or cicks of links raise the chances of accounts being compromised or abused. The lack of proper cybersecurity exposes women to unauthorized access, blackmail, and identity theft.
- **Weak Law Enforcement and Minimum Reporting:** Many females are afraid to report cybercrimes because of the stigma in society, fear of being judged, poor and slow investigation or lack of trust to the authority. Such underreporting gives criminal bravery since they are assured that they can commit crimes without being caught.

- **Anonymity over the Internet:** Criminals can now harass, threaten or exploit women without being detected immediately as there is the capacity to hide or fake identity on the Internet. This anonymity promotes ill acts and complicates the process of tracking the culprits.
- **Social Media Misuse:** The misuse of social media can be characterized as the creation of false accounts, morphing, distribution of obscene material, and abuse messages. Women are often the targets since it is easy to access their photos, posts, and personal details and abuse them.
- **Revenge, Blackmail and Personal Grudges:** It is common with many former partners or people they know well; they can abuse personal messages, photos or videos to threaten, blackmail or even take revenge. The motives of such crimes are mostly based on anger, jealousy, or the willingness to take control.
- **Absence of Intense Supervision by the Social Media sites:** Despite the fact that social media sites have reporting features, they do not react in a fast or efficient manner and consequently the malicious content or the impersonated accounts can remain open. Delay in the response of platforms compounds the risk and effects of cybercrimes against female users.
- **Increased Dating App Use and Online Friendships:** personal information can be abused, a partner can turn in, or be blackmailed once one trusts strangers on a dating app or social media. Women are prone to fall prey of cyber harassment or exploitation when online relationships become abusive or manipulative.

Challenges in Addressing Cybercrime Against Women

Cyber-violence perpetrated against women has not been sufficiently addressed due to the presence of laws since law does not recognize the distinct psychological and social damages of gender-based cyber-violence (Deo & Singh, 2022). The courts and law-enforcement do not have specific training in digital evidence, resulting in low conviction rates, whereas the pace of development of AI, the dark web, and cross-border activity surpasses legal frameworks (Awasthi et al., 2023). There is also a problem of jurisdictional gaps and lack of coherent international cooperation that also allows the perpetrators to go unpunished resulting in an endlessly unmatched cycle of cyber-crime tactics and actionable legal measures. Some of the primary challenges in addressing cybercrime are:

- **Evidentiary Problems & Digital Forensics:** Law-enforcement agencies and their inability to collect or preserve digital evidence are the reason behind their losing cases (Kshetri, 2009). The ephemerality of Internet information, absence of cross-jurisdictional norms, and deficiency of forensic knowledge imply that evidence is often inadmissible in a case, which protects victims of cyber-crime.
- **Capacity and Training Gaps in Law Enforcement:** Police lack the resources to do so, the technology remains out of date, and there are no specialized cyber-investigators. Women are often overlooked in training about unique areas of vulnerability, which results in victim-blaming, poor evidence handling, and encouragement of offenders to act with impunity, which prejudices against reporting (Millar et al., 2021; Przeszlowski et al., 2023).
- **Weaknesses in Judicial Interpretation and Implementation of Cyber-Crime:** The courts fail to conceptualize the gendered nature of cyber-crime and tend to mismatch the application of the law, which fails to find any tangible harm. This translates to low conviction levels, re-victimization, and translation of legislation into effective protection of women (Hughes, 2017; Violin & Nafi, 2022; Panda, 2023).
- **Technological Developments and the New Threats:** The innovations in cyber-attack have been rather rapid, and the new online-platforms are out of control, faster than the laws and the law-enforcement forces. Violators are continuously coming up with new adventures and legal mechanisms and victims are unprepared to deal with them, which undermine the hope of availing justice (Amaral et al., 2022).

Way to Prevent Cybercrime

Cybercrime against women is a serious problem in today's digital world. Here are some steps that can be taken to prevent cybercrime against women.

- **Prompt reporting and registration:** The only ways to discover the full scope of cybercrime are through early reporting and registration.
- **International cooperation through treaties:** The fact that many foreign gangs "servers" are situated outside of India helps them evade discovery. It is necessary to pursue international collaboration through official treaties and unofficial means.
- **Increase awareness**: To ensure that young people, particularly young girls and women, take the necessary safety and security precautions when using the internet, there is a need to raise awareness of cyber safety and security.
- **Better policing:** Regarding the police, we certainly require improved facilities, additional specialized cybercells, police stations, frequent training, and ongoing cooperation with cyber professionals. By enhancing their capacity, forensic labs can gather proof of cyberbullying, threats, morphing, and profiling in a timely manner.
- **Fast trial:** For cybercrimes, a prompt trial would be advantageous. According to the NCRB, just nine cyberblackmail and threat court trials were successfully concluded in 2020, yielding a 66.7 percent conviction rate; 393 similar cases are still outstanding. Prosecutors and judges should receive systematic training on addressing cybercrimes to expedite cases.

Conclusion

Information technology solutions have opened the door to a new world of networking, e-banking, and the internet, which are rising as solutions to cut costs and transform multifaceted economic matters into simpler, faster, resourceful, and time-saving methods of transactions. With the introduction of such facilities cybercrimes, against women have risen. There has to be a campaign to raise awareness about cyber safety and security to encourage women to use the internet responsibly and gradually. The major issue of cybercrime lies in the modus operandi of the cyber-criminal. Women need to be encouraged to speak up when their rights are infringed online. The government must authenticate that the programme to prevent cybercrime against women is functioning effectively and the complainant's privacy must be protected.

Recommendations for Legal and Policy Reforms

The current laws have to combine prevention and prompt response, improve digital backbone, and close the gaps in the legislation in new fields of threats. Unification of international laws will break the borders of jurisdiction and speed up human collaboration across borders. The law-enforcement and judiciary should be provided with specific cyber-skills training, and the population should be educated about cyber-hygiene (in particular, women) and given convenient reporting routes.

- **Reinforcing the IT Act, 2000:** Modify the IT Act to include gender-related offenses such as revenge pornography, cyberstalking, and harassment on the internet which are underrepresented at the moment. Clear clauses will enhance accountability and facilitate prosecution.
- **Optimality of Law-Enforcement Response:** Design strong legal frameworks that regulate the collection and admissibility of digital evidence. Assign dedicated cyber-crime teams with forensic equipment and gender-sensitive skills and require them to be trained constantly in line with the current tactics.
- **Increasing Digital Literacy and Awareness:** Provide extensive education to women and girls, as well as the general audience on safe behavior, privacy settings, and reporting. Similar campaigns against awareness should fight the culture of normalizing online gender violence.
- **The International Cooperation by Strengthening Corporate Social Responsibility:** Enhance inter-country cooperation by harmonizing laws, speeding up the extradition process, and facilitating the exchange of information. Internationalized global standards will ensure that the offenders do not take advantage of the loopholes of jurisdictions.

References:

1. Amaral, I., Simões, R. B., & Poleac, G. (2022). Technology gap and other tensions in social support and legal procedures: stakeholders' perceptions of online violence against women during the Covid-19 pandemic. *El Profesional de La Informacion*. https://doi.org/10.3145/epi.2022.jul.13
2. Awasthi, L., Kumar, A., Awasthi, K. S., Kumar, S., Bajpai, A. K., & Pathak, H. (2023). Cyber Crime Prevention Model Using Artificial Intelligence. *Journal of Chemical Health Risks*. https://doi.org/10.53555/jchr.v13.i4s.1660
3. Balabantaray, S. R., Mishra, M., & Pani, U. (2023). A SOCIOLOGICAL STUDY OF CYBERCRIMES AGAINST WOMEN IN INDIA: DECIPHERING THE CAUSES AND EVALUATING THE IMPACT ON THE VICTIMS. *International Journal of Asia Pacific Studies*, *19*(1), 23. https://doi.org/10.21315/ijaps2023.19.1.2
4. Barak, A. *Sexual Harassment on the Internet*,23(1), SOC. SCI. COMPUT. REV. 77-92 (2005).
5. Borah, U. (2020). Cyber Crime against Women in the Digital ERA: A Breif Indian Scenerio. *International Journal for Research in Applied Science and Engineering Technology*, *8*(7), 615. https://doi.org/10.22214/ijraset.2020.30295
6. Chudasama, D. *A Comparative Study on Cyber Crime, Security, and Law*, 8(2), INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND SOFTWARE ENGINEERINGIJISSE.15-20,16 (2022).
7. CIVILSDAILY, https://www.civilsdaily.com/news/how-to-control-cyber-crime-against-women/ (last visited Sep. 3 2023).
8. Deo, N., & Singh, P. A. (2022). *Cybersecurity and Sustainable Development* (p. 188). https://doi.org/10.55662/book.2022ccrs.009
9. Dhawesh Pahuja, *"Cyber Crimes and The Law"*, LEGAL INDIA, (July .17,2017), http://www.legalindia.in/cyber-crimes-and-the-law.
10. Dhruti M Kapadia**,** *Cyber Crimes Against Women and Laws In India*, LIVELAW (Feb. 26, 2019), https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/.
11. Fatima, H. and Husain J, *Cyberlaw for sexual crimes*,6 (1), INDIAN JOURNAL OF HEALTH, SEXUALITY & CULTURE(IJHSC),22-28,24 (2020).
12. Gius, C. (2023). (Re)thinking gender in cyber-violence. Insights from awareness-raising campaigns on online violence against women and girls in Italy. *Media Education*, *14*(2), 95. https://doi.org/10.36253/me-14896

13. Gupta, S. and Jaggarwal S, *A Descriptive Study on Cyber Crimes Against Women with Reference to Cyber Security Law*, SHODHASAMHITAUGC CARE GROUP 1, IX ISSUE- 12 (III),31-43,36 (2022)**.**
14. Halder, D. and Jaishankar, C*ybercrimes against women in India: Problems, perspectives and solutions*, 3(1), TMC ACADEMIC JOURNAL, 48-62(2008).
15. Hughes, C. (2017). *Legislative Wins, Broken Promises: Gaps in implementation of laws on violence against women and girls*. https://doi.org/10.21201/2017.9163
16. KASPERSKY, Available at https://www.kaspersky.co.in/resource-center/threats/what-is-cybercrime (last visited Sep. 9 2023).
17. KPMG IN INDIA, Cybercrime survey report, (2014)
18. Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, *52*(12), 141. https://doi.org/10.1145/1610252.1610288
19. Kumar, P. N. V. *Growing cybercrimes in India: A survey*, *Proceedings of 2016* INTERNATIONAL CONFERENCE ON DATA MINING AND ADVANCED COMPUTING, SAPIENCE, 246-51((2016). https://doi.org/10.1109/SAPIENCE.2016. 7684146
20. Kumar, s. and Priyanka, *Cyber Crime Against Women: Right to Privacy and other Issues,*5 (**5**), JOURNAL OF LEGAL STUDIES AND RESEARCH,154 – 166,156(2019).
21. Lazarus, S. (2019). Just Married: The Synergy between Feminist Criminology and the Tripartite Cybercrime Framework. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3718426
22. Millar, K., Shires, J., & Tropina, T. (2021). *Gender Approaches to Cybersecurity: Design, Defence and Response*. https://doi.org/10.37559/gen/21/01
23. NORTON, http://us.norton.com/cybercrime-definition (last visited Aug.15,2023).
24. Panda, S. (2023). Towards a Cyberfeminist Framework for Addressing Gender-Based Violence in Social Media. In *Advances in human and social aspects of technology book series* (p. 108). IGI Global. https://doi.org/10.4018/978-1-6684-8893-5.ch008
25. Panwar, K. and Sihag, V.K, *Changing forms of Cyber Violence against Women and Girls*. THE INDIAN POLICE JOURNAL*,* 111-120,117, (2020).
26. PARAMESWARARAO, S., LAKSHMI, B. B., CHIRANJEEVI, P., & SASIDHAR, M. (2021). *AUTOMATIC METHOD TO CLASSIFY CYBER CRIME INCIDENT USING ARTIFICAL INTELLIGENCE AND DEEP LEARNING APPROACHES*.
27. PricewaterhouseCoopers (PwC), "Economic Crime Survey India Report, (2011).
28. Przeszlowski, K., Guerette, R. T., & Sudderth, L. K. (2023). The Role and Impact of the Use of Information Technologies by Police in Response to Violence against Women. *International Journal of Environmental Research and Public Health*, *20*(12), 6125. https://doi.org/10.3390/ijerph20126125
29. Sarmah, A., Sarmah, R. and Baruah, A.J, *A brief study on cyber-crime and cyber laws of India*, 4 (6), Int Res J Eng Technol,1633–1640(2017).
30. Singh, V., & Gautam, D. R. (2022). *Cyber Crime, Security and Regulation in India* (p. 147). https://doi.org/10.55662/book.2022ccrs.005
31. VANGIE BEAL "definition of Cyber-crime". Retrieved 24th October 2015, http://www.webopedia.com /TERM/C/cybercrime.html.
32. Verma, V. *Importance of Cyber Law in India*, LEGAL SERVICE IN INDIA, (September .6 2023) https://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html.
33. Violin, G., & Nafi, Y. K. (2022). Protection of Online Gender-Based Violence Victims: A Feminist Legal Analysis. *The Indonesian Journal of Socio-Legal Studies*, *1*(2). https://doi.org/10.54828/ijsls.2021v1n2.6