INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBERCRIME AGAINST WOMEN IN INDIA: A CRITICAL ANALYSIS OF CURRENT SITUATIONS

AUTHOR - MR. MD JIYAUDDIN, ASSISTANT PROFESSOR OF LAW AT VEL TECH RANGARAJAN DR. SAGUNTHALA R&D INSTITUTE OF SCIENCE AND TECHNOLOGY

BEST CITATION - MR. MD JIYAUDDIN, CYBERCRIME AGAINST WOMEN IN INDIA: A CRITICAL ANALYSIS OF CURRENT SITUATIONS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 4 (4) OF 2024, PG. 217-2226, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

In India, cybercrime is a problem that is expanding quickly and has a big effect on women. Human rights and the right to privacy are violated when violence against women occurs; this is not a recent development. In Indian history, it always takes on new forms from time to time. Many feminists have battled for women's empowerment in society and against violence against them over time, yet the victim's exploitative existence will always exist. The term "cybercrime" refers to a wide range of illegal behaviours wherein computers or networks are utilised as a weapon, a target, or a location. Technology advancements have resulted in a sharp rise in cybercrimes and the victimisation of women online. According to the study online harassment, cyberstalking, revenge pornography, cyber defamation, sexual abuse, cyber extortion, cyber bullying, cybersex trafficking, email misrepresentation and phishing are the most frequent cybercrimes against women in India. Because victims are unaware of their legal alternatives and do not trust law enforcement to properly investigate and punish these offences, many crimes frequently go unreported. People are seriously threatened by cybercrimes. Women are the primary victims of this emerging type of crime, which is a global issue. The author examines internet security flaws and cybercrimes against women in this article. The threat of cybercrime to economic and national security are growing. The Digital Personal Data Protection Act, 2023 establishes guidelines for safeguarding personal data, including securing consent before using it, restricting data collecting, and guaranteeing data accuracy. People also have the right to raise complaints, seek corrections, and receive information. The statute does, however, release the government from some restrictions on the use of data processing for law enforcement. With an emphasis on cybercrimes against women, the Ministry of Home Affairs runs the National Cyber Crime Reporting Portal, which allows residents to file complaints about any kinds of cybercrime.

KEYWORDS: Cybercrime, Human Rights, Right to Privacy, Global Issue Investigate, Digital Personal Data Protection.

I. INTRODUCTION

As technology has grown more and more integrated into our daily lives, cybercrime has become a serious danger to society and other unlawful activity conducted using the internet or other digital technology is referred to as cybercrime. From financial fraud to cyberbullying, hacking, and online harassment, cybercrime encompasses a wide range of offences. Regretfully, in India, where cybercrimes against women have drastically escalated in recent years, women have been disproportionately impacted by cybercrime.[236] Women in India suffer greatly from cybercrime in terms of their physical and emotional well-being. Cyberbullying and online harassment

[236] S. Jaspreet, *VIOLENCE AGAINST WOMEN IN CYBER WORLD: A SPECIAL REFERENCE TO INDIA*, 4(1), International Journal of Advanced Research in Management and Social Sciences, 60, 68-72 (2015).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

have grown commonplace in India due to the growth of social media and internet platforms, particularly targeting women. Threats from cyberspace, such as identity theft, revenge pornography, and stalking, can cause emotional anguish and serious mental suffering for women. India is among the top five nations in the world for cybercrime, which raises serious concerns about the country's present cybersecurity situation. There are still major loopholes in India's cybersecurity implementation, despite the government's attempts to fortify cybersecurity legislation and regulations. A further factor aggravating the issue is the general publics and law enforcement authorities' ignorance of cybersecurity. Furthermore, it is difficult to effectively address the problem because of the rise in cybercrimes brought on by the growing use of technology and the internet.[237]

Cybercrime is a worldwide issue. Technology has led to an increase in cybercrime and the victimisation of women, which is a serious danger to an individual's overall security. Despite the fact that India is among the very few nations that have passed the Information Technology Act, 2000.Women are the most affected victims in this age of technological advancement. These days, digital intervention that is, computer technical interferences start and ends every aspect of existence. As a result, both the positive and negative aspects are shown. The state of violence against women is getting worse every day due to its various manifestations. Cyber violence is a new kind of violence against women that has emerged as a result of technological advancements. India has a high rate of online violence against women, and it is thought that this number is rising. A new type of violence against women that is made possible by the internet and information technology is known as cyber violence.[238]

Women are more likely than males to become victims in cyberspace, and the majority of them get emails from guys they don't know that include unsettling information or texts, friend requests, etc., which might be the product of data mining. Many women who don't mind sharing their accounts and passwords with their boyfriends or spouses are harassed by their former partners, who take advantage of them by posting their images on websites that go viral, blackmailing them, and using cyberspace to exact revenge for breaking romantic commitments, among other things. In India, impersonation, emotional cheating, and creating cloned personas to victimise people online are all on the rise. Cyber victimisation is also a result of a lack of understanding. Although 75% of victims are said to be female, these numbers are based primarily on conjecture. Since most crimes of this kind are not recorded, pose no obvious physical danger, and are not clearly defined or carried out correctly, the precise numbers are really impossible to determine. This explains the surge in cybercrimes against women.[239]

II. IMPACT OF CYBER-CRIME

Women are the most affected victims in this age of technological advancement. These days, digital intervention that is, computer technical interferences start and ends every aspect of existence. As a result, both the positive and negative aspects are shown. Cybercrime is a worldwide issue. Technology development, cybercrime, and female victimisation are all on the rise, and they represent a serious risk to an individual's overall security. The increasing problem of cybercrime in cyberspace puts people's privacy and personal security at risk. The largest network and information system in the world is the internet.[240] With its constantly growing user base, Internet use statistics highlight the consequences of telecom

[237] J. Monika, *VICTIMIZATION OF WOMEN BENEATH CYBERSPACE IN INDIAN* UPBRINGING, Bharati Law Review, 1, 3-5 (2017).
[238] S.C. Tripathi, Women and Criminal Law (Central Law Publication, Prayagraj, 3rd Edition 2021).
[239] Y. Harish, *UNVEILING THE DARK SIDE OF CYBERSPACE: A STUDY OF CYBER CRIMES AGAINST WOMEN IN INDIA,* 11(10), IJFANS, 3408, 3414-3418 (2022).
[240] Id 1.

infrastructure upgrades as they continue to spread into smaller areas. These days, the Internet is a component of the globalisation process that is clearly erasing old realities and certainties and bringing with it both new opportunities and difficulties related to living in a small globe. Human civilisation has benefited from the internet. The internet has brought individuals together all across the world. A fundamental aspect of human nature is the curiosity to learn about the unknown. The desire to learn more about the people who live on Earth has intensified the desire to find the untraversed route. As a result of this, the cyber world has emerged.[241]

III. TYPES OF CYBERCRIME AGAINST WOMEN

Email harassment:

Cyber harassment refers to the act of sending threatening emails or messages, or assuming a false identity and creating a website or profile with the intention of harassing a specific person. In India, it is among the most prevalent types of cybercrime directed against women. It's a lot like sending unsolicited letters. It encompasses bullying, threatening, blackmailing, and even email cheating. Despite being comparable to letter harassment, e-harassment frequently causes issues when it is submitted from a phoney identity. Women may experience severe emotional distress, worry, and terror as a result, feeling exposed and insecure.[242]

Staking:

Stalking is the act of looking for someone. Cyberstalking is what happens when it is done online, although it may also be done in person. Another form of cybercrime that Indian women experience is cyberstalking. It is used to describe a pattern of persistent online harassment that includes tracking, observing, or following someone's online activities. False allegations or factual claims may also fall under this category. Social media, emails, chat apps, and other digital platforms are used by cyber-stalkers to follow and harass their targets.[243]

Cyberbullying:

Cyberbullying is described as bullying someone online, including through dating apps, social media, and online gaming, with the intention of threatening or humiliating the target. Among young girls and women in particular, it is one of the most prevalent types of cybercrime against women. Teenage children are the most commonly targeted demographics for cyberbullying, which is frequently a gender-neutral offence that can be committed against both men and women. The targeted individual is frequently harassed due to his appearance, physique, family, race, religion, fashion sense, demeanour and financial situation.

Cyber Hacking:

In this type of cyberviolence, specific targets are selected in order to hack their profiles and use their personal data for malevolent ends. The hacker could even send out open invites for the profile owner to have sex at her residence. Sections 379 and 406 of the Indian Penal Code but as per the Bharatiya Nyaya Sanhita, 2023 sections 303 and 316, sections 43(a) and 66 of the IT Amendment Act, 2008, respectively, apply for punishment following a violation of the law pertaining to cyber hacking. In accordance with the IT Act, the accused faces up to three years in prison, a fine of five lakh rupees, or both if the offence is proven. With the consent of the recognised court where the prosecution of the offence is ongoing, the offence is cognisable, compoundable, and subject to bail. Any magistrate may try the case.

[241] S. Rajat & M. Mishra, *A SOCIOLOGICAL STUDY OF CYBERCRIMES AGAINST WOMEN IN INDIA: DECIPHERING THE CAUSES AND EVALUATING THE IMPACT ON THE VICTIMS*, 19(1), IJAPS, 23, 33-39 (2023).
[242] S.R. Myneni, Law Relating To Women (Asia Law House, Hyderabad, 3rd Edition 2013, Reprint 2015).
[243] Ibid.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Cyberpornography:

The biggest hazard to female internet users is cyberpornography. Pornographic websites and magazines that use computers to publish and print their content as well as the Internet (to download and distribute pornographic images, photographs, texts, etc.) would fall under this category. Crimes like pornography, particularly cyber porn, have been made easier by the internet. Nowadays, pornographic content may be found on over half of all websites. Because cybercriminals exploit pictures of women and alter them with naked images, this becomes perilous for a woman's integrity. images or videos, and those images or videos solely show one woman.

Cyber Defamation:

Cyber defamation is a tort that occurs when someone spreads untrue information about another individual using computers and the internet. It happens when people start posting pornographic or libellous statements on the many social networking sites that are accessible through the online platform. Because a user's bulletin board is accessible to all users, anybody can post a disparaging comment, and it will be seen by everyone. The words cyber smearing and cyber defamation are interchangeable.

Cyber Grooming:

Cyber grooming is the practice of befriending a young person online with the intention of arranging for sexual meetings between the two of them. It is not uncommon for an adult to make an internet buddy with the intention of later sexually abusing, exploiting, or trafficking the kid. Gaining the trust of the child and obtaining sensitive and private information from them usually sexual in nature, such as sexual conversations, pictures, or videos are the main goals of cyber grooming. The information is then used to blackmail or threaten the child into supplying more inappropriate content.[244]

IV. LEGAL FRAMEWORK OF LAWS AIMED AT PREVENTING CYBERCRIME AGAINST WOMEN

The Indecent Representation of Women (Prohibition) Act 1986 should be amended to cover virtual environments, since the IT Act 2000 and IT Rules 2021 offer a legal foundation for punitive actions against offenders. This proposal has been before Parliament for almost ten years. Furthermore, offline offences against women are purportedly given more weight by Indian courts than internet ones. When someone is charged with both online and offline charges, there is allegedly a propensity to concentrate more on the offline offences. If such an imbalance exists, it should be corrected so that justice is administered equitably regardless of the location of the offence.[245]

All transactions and activities conducted through electronic communication now have legal status in India thanks to the passage of the Information Technology Act 2000. Digital contracts, digital property, and digital rights are all covered under the Act. It is a criminal to break any of these laws. The Act stipulates severe penalties for these offences. The penalties have been further strengthened by the Information Technology (Amendment) Act, 2008 (Act 10 of 2009). Certain types of cybercrimes may result in life in jail and fines of up to Rs. 10 lakhs. If a computer, computer system, or computer network is damaged due to a virus, service interruption, etc., impacted individuals may be eligible for compensation up to Rs. 5 crores. India is one of the few nations that passed an IT Act to tackle cybercrimes, yet this Act does not address concerns pertaining to women.[246]

[244] A. Sarma & Shrushti, Panic room? Towards a safer cyberspace for women 2024, https://www.orfonline.org/expert-speak/panic-room-towards-a-safer-cyberspace-for-women (last visited Oct. 02, 2024).

[245] P. Tanmay, Empowering Women in Cyberspace 2022, https://www.legalserviceindia.com/legal/article-11912-empowering-women-in-cyberspace.html (last visited Oct. 02, 2024).

[246] Women and Cybersecurity: Creating a More Inclusive Cyberspace 2022, https://www.worldbank.org/en/events/2022/04/26/women-and-

- **Section 66A**: This section covers transmitting inflammatory communications through communication services, creating irritation, etc., or sending an email that misleads or deceives the recipient about its origin a practice known as IP or email spoofing. These offences carry a maximum sentence of three years in jail or a fine.
- **Section 66B**: Theft of a computer resource or communication equipment, with a maximum sentence of three years in prison and a fine of one lakh rupees, or both.
- **Section 66C:** Electronic signatures and other forms of identity theft, such as using someone else's password or electronic signature, are covered.
- **Section 66D**: Anyone found guilty of cheating by utilising a computer resource or communication device faces up to three years in jail of any kind and a fine of up to one lakh rupees.
- **Section 66E**: Violation of Privacy: Disseminating or publishing someone else's private information without that person's permission, etc. Three years in jail, a fine of two lakh rupees, or both might be the punishment.
- **Section 66F**: Cyberterrorism is the deliberate attempt to undermine the nation's unity, integrity, security, or sovereignty by preventing anybody who is authorised from using a computer resource or by trying to breach or gain unauthorised access to one. Publication or transmission of pornographic materials via electronic means is covered by Section 67. The ITA Act of 2008 expanded the previous provision of the law to include child pornography and the keeping of records by intermediaries.

cybersecurity-creating-a-more-inclusive-cyber-space (last visited Oct. 05, 2024).

- **Section 72:** Penalties for violating confidentiality and privacy included confidentiality diaries.[247]

V. BHARATIYA NYAYA SANHITA'S PROVISIONS ON CYBERCRIMES AGAINST WOMEN

Sexual harassment: Section 75. (1) A man who commits any of the following acts: (i) physical contact and advances involving unwelcome and explicit sexual overtures; (ii) a demand or request for sexual favours; (iii) showing pornography against a woman's will; or (iv) making sexually coloured remarks is guilty of sexual harassment.[248]

Voyeurism: Section 77: Anyone who witnesses or records a woman performing a private act in a situation where she would typically expect to be unobserved by the perpetrator or by anyone else acting on the perpetrator's behalf, or who shares such footage, faces imprisonment of any kind for a minimum of one year, but up to three years, and a fine. In the event of a second or subsequent conviction, the punishment is imprisonment of any kind for a minimum of three years, but up to seven years, and a fine.[249]

Stalking: Section 78. (1) A man is guilty of stalking if he— (i) follows a woman and contacts, or makes repeated attempts to contact a woman to establish a personal relationship, even when the woman clearly shows no interest in him; or (ii) keeps tabs on a woman's use of the internet, email, or any other electronic communication.

Word, gesture or act intended to insult modesty of a woman: Section 79. Whoever, intending to insult any woman's modesty, utters any words, makes any sound or gesture, or exhibits any object in any form with the intent that such word or sound be heard, or that such gesture or object be seen, by such

[247] G.B. Reddy, Women & The Law including Law Relating to Children (Lex Worth, Gogia Law Publication, 10th edu., 2021).
[248] Vaishali, Bharatiya Nyay Sanhita & provisions regarding cyber-crimes, 2024 https://www.linkedin.com/pulse/bharatiya-nyay-sanhita-provisions-regarding-cyber-shintre-bhagwat69fjf#:~:text=Whoever%20has%20in%20his%20possession,Sanhita%2C%20be%20punished%20with%20imprisonment (last visited Oct. 04, 2024).
[249] Ibid.

woman, or intrudes upon her privacy, shall be punished with simple imprisonment for a term of up to three years, as well as a fine.

Organised crime: Section 111(1) Any continuing unlawful activity, including kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offence, cybercrimes, trafficking of persons, drugs, weapons, or illicit goods or services, human trafficking for prostitution or ransom, by any person or group of persons acting in concert, singly or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate, by use of violence, threat of violence.[250]

Defamation: Section 356. (1) Whoever, by words either spoken or intended to be read, or by signs or visible representations, makes or publishes in any manner, any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.[251]

VI. INDIA'S CYBERCRIMES

Cybercrime is becoming a bigger problem in India, as it is in many other nations. In 2018, 208,456 cybercrimes were reported and investigated. Cybercrimes were recorded in 212,485 cases in the first two months of 2022 alone, which is more than all of 2018. Reports of crime increased more dramatically during the pandemic, rising from 394,499 instances in 2019 to 1,158,208 in 2020 and 1,402,809 in 2021. In India, cybercrime rose by 15.3% in 2022. In addition, the number of Indian websites that have been hacked in recent years has increased. In 2018, 17,560 websites were compromised. There were another 26,121 compromised websites in 2020. In 2021, ransomware attacks affected 78% of Indian organisations, with 80% of those assaults encrypting data. By contrast, the average encryption rate was 65% and the average attack percentage was 66%.[252]

The Ministry of Home Affairs created the I4C, which provides law enforcement with a framework for fighting cybercrime. With 26,049 complaints in 2019, 257,777 in 2020, 452,414 in 2021, 966,790 in 2022, 1,556,218 in 2023, and 740,957 in the first four months of 2024 alone, there has been a noticeable increase in the number of instances reported between 2019 and 2024. The majority of victims fell victim to sextortion, OTP scams, gambling applications, algorithm manipulations, illicit loan apps, and online investment fraud. The I4C documented more than 100,000 instances of investment fraud in 2023. In the first four months of 2024, digital arrests led to 4,599 cases and a loss of Rs 120 crore. During the same year, 20,043 occurrences of trading frauds resulted in a loss of Rs 1,420 crore for hackers.[253]

VII. RECORD PUBLISHED BY THE NATIONAL CRIME RECORDS BUREAU

Crime statistics are compiled and published by the National Crime Records Bureau (NCRB) in their magazine "Crime in India." The most recent study to be released covers 2022. The Annexure contains state-by-state and UT-by-state information on cybercrime cases (using communication devices as a medium or target) for the previous three years, according to statistics released by the NCRB.[254]

I. no	State/UT	2020	2021	2022
1	Andhra Pradesh	1899	1875	2341

[250] The Bharatiya Nyaya (Second) Sanhita, 2023, https://prsindia.org/billtrack/the-bharatiya-nyaya-second-sanhita-2023 (last visited Oct. 04, 2024).
[251] Ibid.
[252] R. Ranjan & J. Gulati, CYBER CRIMES AGAINST WOMEN IN INDIA FROM COVID TO THE PRESENT ERA 2023,
[253] A. Pathak & P. Tripathi, *DIGITAL VICTIMIZATION OF WOMEN IN CYBERSPACE: AN ANALYSIS OF EFFECTIVENESS OF INDIAN CYBER LAWS*.
[254] J. Ramanath, Crime in India: A Critical Review of Data Collection and Analysis 2024, https://www.orfonline.org/research/crime-in-india-a-critical-review-of-data-collection-and-analysis (last visited Oct. 05, 2024).

2	Arunachal Pradesh	30	47	14
3	Assam	3530	4846	1733
4	Bihar	1512	1413	1621
5	Chhattisgarh	297	352	439
6	Goa	40	36	90
7	Gujarat	1283	1536	1417
8	Haryana	656	622	681
9	Himachal Pradesh	98	70	77
10	Jharkhand	1204	953	967
11	Karnataka	10741	8136	12556
12	Kerala	426	626	773
13	Madhya Pradesh	699	589	826
14	Maharashtra	5496	5562	8249
15	Manipur	79	67	18
16	Meghalaya	142	107	75
17	Mizoram	13	30	1
18	Nagaland	8	8	4
19	Odisha	1931	2037	1983
20	Punjab	378	551	697
21	Rajasthan	1354	1504	1833
22	Sikkim	0	0	26
23	Tamil Nadu	782	1076	2082
24	Telangana	5024	10303	15297
25	Tripura	34	24	30
26	Uttar Pradesh	11097	8829	10117
27	Uttarakhand	243	718	559
28	West Bengal	712	513	401
	TOTAL STATE(S)	**49708**	**52430**	**64907**
29	A&N Islands	5	8	28
30	Chandigarh	17	15	27
31	D&N Haveli and Daman & Diu	3	5	5
32	Delhi	168	356	685
33	Jammu & Kashmir	120	154	173
34	Ladakh	1	5	3
35	Lakshadweep	3	1	1
36	Puducherry	10	0	64
	TOTAL UT(S)	**327**	**544**	**986**
	TOTAL (ALL INDIA)	**50035**	**52974**	**65893**

VIII. CONSTITUTIONAL PROTECTIONS AGAINST WOMEN

The right to privacy, which is a fundamental component of individual liberty and dignity, is safeguarded by Article 21 of the Indian Constitution. It declares that no one's life or personal freedom may be taken away from them without following the proper legal procedures. Article 21, which also safeguards other rights including the right to life, the right to education, and the right to a clean environment, includes protection for the right to privacy. The right to privacy is a fundamental component of life and individual liberty, according to the Supreme Court's interpretation of Article 21. The Supreme Court has also recognised that

reasonable limitations may be placed on privacy, which means that it is not absolute. The triple criteria of legality, need, and proportionality must be met by any restrictions on the right to privacy.[255]

The Supreme Court acknowledged its tacit existence in other constitutionally protected fundamental rights, including Article 21's right to life and personal liberty. The Supreme Court established the compelling state interest test in the seminal decision of Gobind v. State of MP (1975, AIR 1975 SC 1378, (1975) 2 SCC 148), highlighting the need for private rights to give way to greater state interests only when they are clearly justified. Another significant turning point was reached in the 1997 PUCL v. Union of India case, sometimes known as the telephone tapping cases (AIR 1997 SC 568, (1997) 1 SCC 301). The Supreme Court's clear recognition of people's right to privacy regarding the content of their phone conversations in this case strengthened the Constitution's recognition of privacy rights. However, the legal acknowledgement of privacy as a basic right came about in 2017 with the landmark judgement of Justice K.S. Puttaswamy v. Union of India.[256] The protection of privacy was firmly established by the Supreme Court's majority ruling under Article 21 that it is an essential component of life and personal liberty.

It emphasised how privacy is linked to other fundamental rights including equality, freedom of speech and expression, and religious freedom. The ruling acknowledged that privacy is vital but also emphasised the need for balanced regulation, recognising that, like other rights, privacy can be subject to reasonable limitations. Any restriction on the right to privacy must meet the three requirements of proportionality, need, and legality, according to the statement. These rulings have established a strong basis for defending privacy rights against intrusions by both state and non-state actors, guaranteeing that people's private interests are appropriately recognised and protected.[257]

State of Tamil Nadu v. Suhas Katti,[258] in this case the conviction was obtained within seven months of the FIR being filed, making it a milestone case under the Cyber Law regime. The victim's family friend, the accused, planned to wed her, but she ended up marrying another guy, leading to a divorce. The accused convinced her once more after her divorce, and he used the Internet to harass her since she was reluctant to marry him. The accused created a phoney email account in the victim's name and posted offensive, vulgar, and vexing content about the victim. Sections 469 and 509 of the Indian Penal Code, 1860, as well as Section 67 of the IT Act, were utilised to submit a charge sheet against the defendant.

In accordance with Sections 469 and 509 of the Indian Penal Code, 1860, as well as Section 67 of the IT Act, the accused was found guilty by the Additional Chief Metropolitan Magistrate, Egmore. Under Section 469 of the IPC, the accused faced two years of rigorous imprisonment and a 500 rupee fine; under Section 509 of the IPC, he faced one year of simple imprisonment and a 500 rupee fine; and under Section 67 of the IT Act, he faced two years of rigorous imprisonment and a 4,000 rupee fine.

Shreya Singhal v. UOI,[259]In this case, the Supreme Court heard a challenge to the legality of Section 66A of the IT Act. After posting allegedly rude and unpleasant remarks on Facebook on the entire shutdown of Mumbai following the death of a political leader, two ladies were detained under Section 66A of the IT Act. The IT Act's Section 66A punishes anybody who uses a computer resource or communication to spread offensive or misleading material that annoys, inconveniences, endangers, insults, incites hate,

[255] S. Kumar & Priyanka, Distinguish between compulsory winding up and voluntary winding up, 5(5), JOURNAL OF LEGAL STUDIES AND RESEARCH, 154, 157-165 (2019).
[256] K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
[257] Id 7.
[258] State of Tamil Nadu v. Suhas Katti CC No. 4680 of 2004
[259] Shreya Singhal v. UOI (2013) 12 SCC 73.

causes harm, or incites malice. Following their detention, the ladies filed a petition contesting Section 66A of the IT Act, arguing that it violates their right to free speech and expression.

The Supreme Court used three ideas discussion, advocacy, and incitement to support its ruling. The freedom of speech and expression, it was noted, is based on the simple act of discussing or even advocating for a cause, regardless of how unpopular it may be. Section 66A was found to have the power to censor all forms of communication and to make no distinction between mere discussion or advocacy of a cause that some people find offensive and incitement by such words that results in a causal connection to public disorder, security, health, and other issues. In answer to the inquiry on whether Section 66A seeks to shield people from defamation, the Court held that the statute forbids offensive remarks that could irritate a person without harming his or her reputation. However, the Court also pointed out that there was a discernible distinction between material conveyed online and through other speech channels, meaning that Section 66A of the IT Act does not violate Article 14 of the Indian Constitution. Additionally, because procedural unreasonableness is illegal on substantive grounds, the Apex Court did not even evaluate this issue.[260]

CONCLUSION

Women are being harassed and abused online in a variety of ways, and cybercrimes against them have increased in frequency in India in recent years. These crimes can have serious repercussions, including financial loss, reputational harm, and emotional distress. Even though India has a rather robust legislative framework to combat cybercrimes against women, police enforcement and the judicial system nevertheless confront a number of obstacles in their efforts to combat these crimes. The Indian government has taken a number of steps and put laws in place to prevent and report cybercrimes against women in an effort to address this problem. Nonetheless, it is imperative to address the root causes of these crimes, which include patriarchal attitudes, gender-based abuse, and a lack of knowledge about cyber security. It is necessary to arrange workshops and seminars on cyberspace education for this reason. It is important for women to engage in these kinds of activities. Again, though, since cleaning begins at home, people need to shift their perspectives about women and cultivate a spirit of solidarity. In order to make India a great country, let's endeavour to grant women the status and position they so richly deserve. Swami Vivekananda once remarked, "The nation which does not respect women will never become great now and nor will ever in future."

Furthermore, it is important to remember that only enforcing fines or jail sentences as sanctions is insufficient to prevent cyber victimisation. In order to further harass the victims, it is possible to track subscriber usage by creating false identities and using social media or other online platforms. When it comes to monitoring subscribers' online activity by creating false identities and using social media or other websites to further harass victims, online service providers such as WhatsApp, Google, Yahoo, Facebook, Instagram, and Twitter all of which are based in the United States are essentially careless. To protect themselves from such crimes and report them to the appropriate authorities, people and students need to receive general training and learn how to utilise applications and software. Therefore, depending on how it is used, the internet may be either a blessing or a curse. Although it may present countless opportunities and allure, one must constantly be mindful of their privacy and rights and understand how to utilise these applications and technologies as efficiently as possible.

[260] M P Jain, *Indian Constitutional Law* (Lexis Nexis, 8th edn., 2018).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

SUGGESTIONS

- The campaign to raise awareness of cybercrimes: From the very beginning, schools, colleges and other educational institutions should launch an awareness campaign about cybercrimes such as economic and stalking cheating, defamatory activities, misuse of social media and emails, virtual rapes, cyber pornography, email spoofing and more. These efforts have the potential to effectively halt cybercrimes.
- The workshops and seminars for a better understanding of cyber victimisation: To discuss the legal and illegal aspects of cyber conduct among adults of both sexes, education institutions, clubs, corporate offices, awareness campaigns, and NGOs, police, lawyers, and social workers must be invited. It is necessary to promote the direct reporting of cybervictimization at all levels to law enforcement and non-governmental organisations that combat cybercrime. Second, in order for police officers to better comprehend these types of victimisations and respond to complaints promptly, courses and seminars must be held for them. NGOs, legal and academic professionals, and others must be invited to these workshops and seminars.
- The 'National Cyber Crime Reporting Portal' (https://cybercrime.gov.in) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber-crimes, with special focus on cyber-crimes against women and children. Cyber-crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.
- The "Cyber Crime Prevention against Women and Children (CCPWC)" Scheme, the Ministry of Home Affairs has given the States and Union Territories financial support totalling Rs. 122.24 crores to help them build their capacity. Some of the activities include hiring junior cyber consultants, establishing cyber forensic and training laboratories, and providing training to public prosecutors, judicial officers, and LEA staff. So far, 33 States and Union Territories have established cyber forensic and training facilities. Over 24,600 LEA employees, judges, and prosecutors have received training on cybercrime awareness, investigation, forensics, and other topics thus far.
- In order to raise awareness of OGBV and associated crimes, train LEAs, and enhance cyber forensic skills, the government also operates the "Cybercrime Prevention against Women and Children" (CCPWC) program. The government's efforts to support women's safety online continue to be anchored by advocacy and capacity building, which are frequently conducted in collaboration with digital platforms and civil society organisations (CSOs).