Page 697 - 711

DOI: *https://doij.org/10.10000/IJLMH.112310*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 6

2021

A Study on Online Violence against Women during Covid 19 Pandemic with Special Reference to India

AAKRITI PANDEY MISHRA[1]

ABSTRACT

Amid public health and economic chaos, a major problem which is presently looming in the shadow of the Covid-19 pandemic is the growing incidences of violence against women (VAW). This paper attempts to provide an understanding of rising online violence which Indian women are facing during the global Covid 19 pandemic era. The dangers of cybercrime have existed for many years during the age of internet ever since computers became commonplace and accessible to the public, but during the Corona pandemic, the rise in gender-based violence online has become alarmingly more rampant and serious. The percentage of the women population connected to the Internet and the amount of time spent online during pandemic, has provided even more opportunities and impetus for cybercriminals to harm women with very little effort and resources. With the increasing risk of harassment, the cyber space is becoming more toxic for women. In an increasingly digital online world, cyber crimes not only belittle, demean, intimidate women rather it drives women out of cyberspace which is against the worldwide mission of women empowerment. After such untoward incidents, many women either delete their social media accounts or reduce the activities of posting and expressing their personal views because of fear of further harassment. This results in driving women away from all the opportunities of better world and a better life that the internet promises to offer. It is indeed a human rights issue and needs to be addressed as such so that we can make progress towards the egalitarian agenda of Sustainable Development Goals 2030. The paper concludes that combating cyber victimization of women requires commitment with multiple stakeholders coupled with technical augmentation and capacity building of law enforcement agencies. Furthermore, the initiative to enhance digital safety awareness is prioritized so that women report such incidents without any fear, get speedy and effective redressal for such complains and exercise their right to be safe and secure in virtual world.

Keywords: *Online Violence against women, COVID 19 Pandemic, Challenges of Criminal Justice System, Social Media Crimes, Sulli Deals.*

[1] Author is a Research Scholar at Dr. Ram Manohar Lohiya National Law University, Lucknow, India.

I. Introduction

COVID-19 pandemic has made a remarkable impact on every aspect of life. With the outbreak of pandemic governments around the world-imposed lockdowns with the aim to contain the spread of novel corona virus. It is the first major pandemic during the period of advanced Information Technology. This has inevitably increased the usage of digital technologies and women's presence in cyberspace for various reasons like health-related procedures, work, studies, jobs, shopping, family and social interactions, entertainment etc. Increased online time provided perpetrators to easily harm women online. UN Women report indicates that cases of online violence against women have increased during the pandemic due to the rising levels of internet use worldwide.[2] Increased time online is linked to increased risks of online harms, ranging from hate speech and harassment to sexual violence and threats. Because of the rise in number of cyber violence cases against women it is deemed to be the "shadow pandemic" by the United Nations. Online Gender based violence against women (Online GBVAW) is defined as any act of GBVAW that is committed, assisted or aggravated in part or fully by the use of information and communication technologies ICTs such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or that affects women disproportionately.[3] When women and girls do have access to the Internet, they face online violence more often than men through a continuum of multiple, recurring and interrelated forms of gender-based violence.[4]

In this internet age, social media has become the part of women's life and hence, it should be a safe and secure space for them. The internet is indispensably important for many reasons like staying in touch with friends, communicating with family, seeking job opportunities, shopping, information exchange, keeping abreast with current issues of national and international importance and learning new skills etc. When any online harassment occurs, women tend to self-censor themselves, meaning, either they leave or significantly reduce the use of social media platforms which only reflects that women are not being able to exercise their right of freedom of expression and right to dignified life as guaranteed under Article 19 & Article 21 of Indian Constitution. Impact of online harassments is grave because it takes mental toll, and women feel unsafe using the cyber space which accessible to everyone. UN statistics indicate that less than 10 percent of women who experience violence and seek help actually report to

[2] EVAW COVID-19 briefs UN Women, https://www.unwomen.org/en/digital-library/publications/2020/04/series-evaw-covid-19-briefs (last visited Nov 1, 2021).

[3] Human Rights Council (2018)

[4] OHCHR Special Rapporteur on violence against women, its causes and consequences Ohchr.org, https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/SRWomenIndex.aspx (last visited Nov 10, 2021)

the police.[5] Majority of women prefer not to seek legal recourse due to prevailing cultures of victim-blaming and shaming. This paper demonstrates how the Covid-19 pandemic increased the likelihood of online violence using a theoretical basis. This theoretical work is supported by media reports from regional news sources documenting the pandemic's effect on online harassing women. While providing an incomplete statistical picture, these types of data are presumably indicative of underlying trends. Additional research will be necessary both during and after the pandemic to better understand how the virus facilitates online violence in India and which measures are effective at preventing or reducing violence. The second part of the present paper highlights the issue of surge in cyber violence cases against Indian women during ongoing Covid 19 Pandemic. The third section highlights the existing and additional challenges faced by criminal justice system especially during the pandemic induced lockdown. In fourth section of the paper an attempt has been made to discuss recent judgements of various High courts dealing with the issue of digital violence. This has been done to emphasise that the judiciary is aware of rising incidences of cybercrimes and therefore taking an active role by way of issuing certain directions to law enforcement agencies so as to make cyber space safer for women. Lastly, paper concludes that there exists is an urgency for India to reform its approach in tackling cybercrimes against women and adopt measures which ensures safety of women in cyberspace.

II. Covid 19 pandemic & online violence against Indian women

Pandemic has led to increase in digital violence as the world turns to remote work and higher Internet usage for virtual socialization. During the Covid-19 pandemic, much of life has transitioned online in regions where Internet is accessible. More Internet usage may therefore lead to more opportunities for women to experience digital violence such as unsolicited pictures, sexist comments, physical threats and stalking. *Online violence can inter alia be in the form of physical threats, sexual harassment, stalking, zoombombing and sex trolling.*[6] Just because it's online does not make the violence any less harmful. In this part of the paper an attempt has been made to indicate the rise in cybercrimes cases against women during Covid 19. This section of the paper is schemed by incorporating data and recent reported cases with the object to substantiate the seriousness of the issue of online violence. This section is further sub divided in two parts 2.1 mainly focuses on quantitative data collected from various reported news, survey, studies conducted by renowned organization working in the field of cybercrimes.

[5] United Nations Economic and Social Affairs (2015)

[6]https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/brief-preventionviolence-against-women-and-girls-and-covid-19-en.pdf?la=en&vs=3049 (last visited Nov 1, 2021)

The objective is to demonstrate the most recent statistics which present the sudden rise in cyber crimes against women during pandemic time. Whereas, 2.2 highlights the two major incidents which took place when India was grappling with the second wave of Covid 19. These reported crimes present gloomy picture of the efficacy of the law enforcement machinery in dealing with cybercrimes against women.

2.1 *Here under is the data which has been gathered to project the incidences of online violence which were committed in various parts of India:*

- According to National Crime Record Bureau 2020 crimes against women dip by 24%, whereas there is 55% rise in cybercrimes in 2020 as compared to 2019.[7] According to the data, cases pertaining to transmitting of sexually explicit act and material accounted for 19 cases in 2019, which increased to 59 in 2020.

- A research study conducted by National Bureau of Economic Research provided that there has been a large increase in the number of cybercrime complaints received by the NCW from red zone districts from April–May 2020. In comparison, orange and green zone districts show smaller increases in the number of cybercrime complaints.[8] Red zone districts had a 184% increase in cybercrime complaints relative to green zone districts in May 2020. Orange zone districts saw a smaller 31% increase in cybercrime complaints relative to green zone districts. This data can be contrasted with the fact that Cyber Crime complaints in red zone districts were lower than green zone districts in May-October 2020. The number of cybercrime complaints also continues to increase in red zone districts until July 2020[9]. By November 2020, the number of complaints decreased to pre-lockdown levels (with the exception of an increase in January 2021). Thus, the data shows an increase in cybercrime during the COVID-19 lockdowns in India, with increases most concentrated in districts that saw the strictest lockdown measures.

- The survey conducted by Plan International[10], revealed in its report that more 58 percent women have faced online harassment or abuse.[11] Most targeted women are threatened with

[7] *The Hindu* (New Delhi 16 September 2021) https://www.thehindu.com/news/cities/Delhi/crimes-against-women-dip-by-24-cybercrimes-see-55-rise-ncrb-data/article36486113.ece (last visited Nov 1, 2021

[8] Saravana Ravindran; Manisha Shah, ***Unintended Consequences of Lockdowns: Covid-19 and the Shadow Pandemic***, https://www.nber.org/system/files/working_papers/w27562/w27562.pdf (last visited July10, 2021)

[9] Hindustan Times https://www.hindustantimes.com/india-news/explained-india-s-lockdown-3-0-in-one-chart-for-red-orange-and-green-zones/story-64r6uIu77tKH2b26Rf00DN.html (last visited Nov 11, 2021)

[10] Abuse and harassment driving girls off Facebook, Instagram and Twitter Plan International, https://plan-international.org/news/2020-10-05-abuse-and-harassment-driving-girls-facebook-instagram-and-twitter (last visited Nov 3, 2021)

[11] Free to be Online Plan International'https://www.plan.de/fileadmin/website/05._Ueber_uns/Maedchenberichte/Maedchenbericht_2020/Free_to_be_online_report_englisch_FINAL.pdf (last visited on September 10, 2021)

physical or sexual violence. These attacks are most common on Facebook, Instagram, WhatsApp, Snapchat, Twitter, and TikTok.

- The Annual Report of National Commission of Women provided that 54 cyber-crime complaints were received online in April this year in comparison to 37 complaints received online in April 2019.[12] 412 genuine complaints of cyber abuse from March 25 till April 25, 2020. Out of these, 396 complaints were serious in nature.[13]

- In Kolkata, the number of cyber-crimes have multiplied especially where women are ending up as victims. These crimes are very personal and try to target the reputation of women. Initiative of creating cyber women helpdesk at the cyber cell police station which would work as a guide/helping hand to women being duped and harassed online. Creating divisional cyber cells to track down criminals and train investigating officers to tackle cyber-crime.[14]

- National Crime Records Bureau 2019 data: Cyber-crimes registered a 63.5% jump as compared to 2018 which includes[15] Motive of fraud: 60.4%, Sexual Exploitation: 5.1%, Causing Disrepute: 4.2%.

- There has been an increase in cyber-crimes against women in the city of Vadodara, Gujarat where social media is one of the key causes of the majority of the complaints filed by women in the state. The Gujarat police provided that "Cases of stalking on social media, tampering with pictures of women with social media profiles, have increased."[16]

- Vineet Kumar, founder and president of Cyber Peace Foundation, said specially the cases of "sextortion" have increased during the lockdown. He further said that there has been a rise in cases where women are getting duped online when they click on malware links which get all their information on phone, turn on the camera and microphone, and capture their intimate moments which are then used for blackmailing.[17]

- The state of Himachal Pradesh has recently reported a huge spike in cyber-crimes especially against women. Miscreants using nude or semi-nude pictures of women to further

[12] The Hindu, https://www.thehindu.com/news/national/andhra-pradesh/cyber-crimes-against-women-on-the-rise/article32399536.ece (last visited on July 21, 2021)

[13] National Commission for Women, Annual Report 2018-19, http://ncw.nic.in/sites/default/files/FINAL%20NCW%20ENGLISH%20ANNUAL%20REPORT%202018-19_0.pdf (last visited on July 21, 2021)

[14] Times of India, https://timesofindia.indiatimes.com/city/kolkata/kolkata-police-help-desk-to-counter-rising-cyber-crimes-against-women/articleshow/80597460.cms (Last visited on July 21, 2021)

[15] Times of India, https://timesofindia.indiatimes.com/india/ncrb-crime-data-2019-cases-registered-up-1-6-crimes-against-women-rise-7-3-cyber-crimes-jump-63-5/articleshow/78394087.cms (last visited on July11, 2021)

[16] Times of India https://timesofindia.indiatimes.com/city/vadodara/social-media-makes-women-more-prone-to-cyber-crime/articleshow/78434864.cms (last visited on July 10, 2021)

[17] "Significant" Increase In Cyber Crimes Against Women During Lockdown: Experts NDTV.com, https://www.ndtv.com/india-news/significant-increase-in-cyber-crimes-against-women-during-lockdown-experts-2222352 (last visited Nov 2, 2021)

blackmail them or using morphed photos of women. Cases of bank fraud (targeting women by luring them with debit/credit card reactivation, online bookings, free Covid-19 test, winning lotteries, zero percent interest loans etc.)[18]

- The research by the United Nations Office on Drugs and Crimes provided reported that there has been an increase in incidents of domestic violence and cybercrime targeting women has also been recorded in districts where lockdown measures were stricter.[19]

- According to the data of National Crime Records Bureau, Maharashtra reported the highest number of cases of cyberstalking/bullying of women for three years in a row. One woman is stalked or bullied on social media every day. Maharashtra also accounted for one-third (1126) of the total 2,051 cyberstalking/bullying cases reported across India in the last 2 years. Andhra Pradesh came second with 184 cases and Haryana third with 97 cases.

- According to Hyderabad Police, over 2,400 cases registered were related to cybercrime which was just 1,393 in 2019. There has been a huge increase in cyber stalking, bullying, and harassment against women.[20]

These statistics are quite alarming and therefore, merit focused and collective attention from Law Enforcement Agencies on an urgent basis. Many complaints were serious ones from women, (and these) ranged from abuse, indecent exposure, unsolicited obscene pictures, threats, malicious emails claiming their account was hacked, ransom demands, blackmail and more.[21] This data suggests that women are being targeted more often and suffer much serious consequences as a result. These statistics must be recognized for what they reveal: just the tip of the iceberg.

***2.2** Major reported incidents of online harassment of which investigation is pending*

2.2. 1.Harassment while seeking online help for Covid

In the times when second wave of Covid19, hit India many people used social media for seeking help. Unfortunately, many women who appealed to the community in good faith revealing their contact details for good Samaritans, faced harassment by unknown men even as

[18] Cyber crime cases spike in Himachal Pradesh, mostly women targeted | Shimla News - Times of India The Times of India, https://timesofindia.indiatimes.com/city/shimla/cyber-crime-cases-spike-in-hp-mostly-women-targeted/articleshow/76988736.cms (last visited Oct 22, 2021)

[19] Unodc.org, https://www.unodc.org/documents/data-and-analysis/covid/Violence_against_women_24Nov.pdf (last visited Nov 2, 2021)

[20] Cybercrime soars in 2020 as hackers take advantage of COVID-19 pandemic; here's how you can protect yourself Jagran English, https://english.jagran.com/india/cybercrime-soars-in-2020-as-hackers-take-advantage-of-covid19-pandemic-heres-how-you-can-protect-yourself-10022015 (last visited Nov 12, 2021)

[21] "Significant" Increase In Cyber Crimes Against Women During Lockdown: Experts NDTV.com, https://www.ndtv.com/india-news/significant-increase-in-cyber-crimes-against-women-during-lockdown-experts-2222352 (last visited Sep 7, 2021)

they were struggling to find an oxygen cylinder, ventilator or hospital bed for Covid-positive family members. Amid medical emergencies they received lewd texts, video calls, from unknown numbers compelling women to switch off their phones.[22] Practically the women who are already under stress of her family members' health found getting the report registered as another hassle.

2.2.2Harassment by Virtual Auction of women

In early July 2021, photographs of more than 80 women were uploaded for virtual auction. GitHub is the web platform that hosted the virtual auction of women by an open source app "SULLI DEALS". These photos were taken from the social media accounts of the women without their consent. The app acted as a platform to advertise these women as "deals of the day". Photographs along with a link to victims Twitter account was also being circulated on the app. Post this, victims started receiving messages containing sexually explicit language, gestures, threats of sexual attacks and even of physical violence. Most of the targeted women were vocal Muslims, including journalists, activists, artists and researchers. The objective behind the app was just to degrade and humiliate women. GitHub, which hosted the app, took it down after public outrage and complaints.[23] Unfortunately, the accused of such heinous acts are not being arrested even after 3 months of reporting. The problem in this case is investigating authorties are facing legal impediments. When the police issued notices under Criminal Procedure Code to GitHub to share the details of the IP address of the web page where photographs of Muslim women were shared, the company responded asking the enforcement agency to take the legal route to approach them under Mutual Legal Assistance Treaty (MLAT). MLAT is an agreement between two or more countries put in place for the purpose of gathering and exchanging information in an effort to enforce laws. Furthermore, enforcing legal route will involve concerned embassy to take legal action. The requested information documents has to be presented to the Ministry of Home Affairs, who will then pass it to the embassy concerned. The legal aid of the embassy then will take it further. This procedure will delay the information by at least a few months. The major problem is that many victims of cyber crimes are left with the feeling that if pre emptive and proactive actions were taken by the investigating authorities then cyber criminals wouldn't have the courage to do something like this again. Regretfully, even after filling of FIR, the investigation progress is sluggish.

[22] https://www.news18.com/news/india/women-face-epidemic-of-online-stalking-harassment-on-seeking-help-in-covid-crisis-3760676.htm (last visited Aug 11, 2021)

[23] Noida: FIR against app that uploaded pictures of women to harass and defame them The Indian Express, https://indianexpress.com/article/cities/delhi/delhi-fir-against-app-that-uploaded-pictures-of-women-to-harass-and-defame-them-7394114/ (last visited September 18, 2021)

Perpetrators take this to their advantage and continue to harass women from one platform to another and causing mental disruptions in women's life.

III. Challenges while tackling online violence

3.1 Existing Challenges with criminal justice system

India is becoming increasingly vulnerable to this menace because of rapid digitization and proliferation of mobile data without matching pace of cyber security and cyber hygiene. Online violence has profound consequence as it affects wellbeing of women and demolishes their self-esteem. Regretfully, governments censor the posts that are critical to them but when it comes to protecting women freedom of expression, they don't bother enough to take immediate actions. Women are frequently targeted for online rape threats, harassment, cyberstalking, blackmail, and other forms of harassment.

The primary laws dealing with cyber crimes in India are the Information Technology Act, 2000 and the Indian Penal Code. Firstly, law does not recognise lot of acts as offences and secondly, law doesn't not prescribe suitable quantum of punishment. Even when the law does prescribe strict rules and harsh punishments the execution and implementation leaves much be desired. Research the world over shows that strong laws on violence act as a deterrent. India needs dedicated legal provisions for protecting women in cyberspace, and data related to women needs to be specifically protected. The current provisions of the IT Act are not adequate. Section 67, 67A and 67B don't specifically cover grooming and handholding of women on the Internet for sex crimes.[24] While addressing cyber crime against women stakeholders of the criminal justice system are facing technical, operational, legal and human resources challenges. There is lack of trained police personnel to effectively investigate these crimes, frequent transfers of the small number of trained personnel leading to incomplete investigations and the lack of standard procedures for seizure and analysis of digital evidence.[25] This is perhaps indicative of the ineffective institutional mechanism for dealing with cybercrimes and shows the need for structural reform. In *Vijesh vs. State of Kerela* Hon'ble Kerela High court also emphasized that *it is high-time for the State Police to bring out a good practise guide for digital evidence, if they intend to tackle cyber crime head on. Officers, who are engaged in*

[24] NCW conducts consultation on amending IT Act to protect women better online The Economic Times, https://economictimes.indiatimes.com/news/politics-and-nation/ncw-conducts-consultation-on-amending-it-act-to-protect-women-better online/articleshow/79549273.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cpps (last visited Oct 22, 2021)

[25] M. Elavarasi1 & N. M. Elango, *Analysis of Cybercrime Investigation Mechanism in India, 10 Ind. J. of Science and Tech. 40, 41 (2017); Arunabh Saikia, Why most cybercrimes in India don't end in conviction, LiveMint (July 29, 2016)*

investigation of cyber crimes, are required to be trained in best practices to tackle the criminal misuse of current and emerging technologies."[26]

3.2. Additional Challenges on criminal justice system during covid 19

The implementation of COVID 19 mitigation measures has created additional challenges for the criminal justice system in responding to gender based violence against women GBVAW[27]. UNODC Coronavirus Disease (COVID 19) response Thematic Brief on gender based violence against women and girls has underlined the following difficulties

- Resources are being diverted away from the criminal justice system towards more immediate public health measures to deal with COVID 19.
- Police and other law enforcement agencies have less time and human resources to respond to incidents of GBVAW, may lack specific plans on how to respond to such incidents during the emergency and are likely to shift priorities
- Towards enforcing quarantine, monitoring social distancing and other related measures. In countries with weak rule of law and existing economic constraints, the focus has shift towards responses to other crime that have increased as a result of economic and social consequences of the responses to COVID 19.
- In many countries, judicial proceedings are suspended and/or postponed, which hampers immediate judicial protection (e. issuance of emergency o r interim measures like protection and restraining orders) and creates a backlog of cases that affects the effectiveness and quality of criminal justice responses to GBVAW in the long run.
- Other services, such as hotlines, crisis centres, shelters, access to a lawyer including through legal aid, and victim protection services may also be scaled back or closed, further reducing access to the few sources of help that women in abusive relationships might have.
- Due to the lockdown policies in place, women and girls may have more difficulties accessing police stations to directly report cases of GBVAW and seek judicial and other forms of protection

IV. CYBER HARASSMENT AND PROACTIVE JUDICIARY

4.1 Directions with regard to de-indexing and de-referencing of offending content

[26] Cybercriminals way ahead of law enforcement officers: Kerala High Court The New Indian Express, https://www.newindianexpress.com/states/kerala/2018/nov/11/cybercriminals-way-ahead-of-law-enforcement-officers-kerala-high-court-1896588.html (last visited Sep 18, 2021)

[27] https://www.unodc.org/documents/AdvocacySection/GBVAW_and_UNODC_in_COVID19_final_7Apr2020.pdf (last visited Nov 22, 2021)

In April 2021 Delhi High Court passed a landmark judgment with set of directions in the issue involving offending content being reposted and republished with multiple websites. In *X v. Union of India* [28] petitioner's photographs were taken from her Facebook and Instagram accounts and had been posted on a pornographic website; and then having been reposted onto other websites and online platforms, amounting to an offence under Section 67 of the IT Act in addition to other offences under the IPC. Cyber crime unit of Delhi Police conveyed its willingness to comply with Court's directions of removing/disabling access to the offending content related to the petitioner, but by reason of technological limitations and impediments, it could not assure the Court that it would be able to entirely efface the offending content from the world-wide-web. While on the other hand, the petitioner complained that even after interim orders for immediate removal of the offending content from the errant website there was blatant disregard of such directions, mischief-makers had redirected, reposted and republished the offending content onto other websites and online platforms, thereby rendering the orders of the Court ineffective. The Court in order to provide an effective and implementable orders in relation to a grievance arising from offending content placed on the world-wide-web issued certain directions so that legal proceedings are not futile.

- The petitioner was directed to furnish in writing to the Investigating Officer of the subject FIR, all available information relating to the offending content, including the Image URL and Web URL pertaining to the offending image files, within 24 hours of receipt of a copy of the judgment, if not already done so;

- The Delhi Police/CyPAD Cell were directed to remove/disable access to the offending content, the Web URL and Image URL of which would be furnished by the petitioner as above, *from all websites and online platforms, forthwith* and in any event within 24 hours of receipt of information from the petitioner;

- A direction was issued to the search engines Google Search, Yahoo Search, Microsoft Bing and DuckDuckGo, to *globally* de-index and de-reference from their search results the offending content as identified by its Web URL and Image URL, including de-indexing and de-referencing all web-pages, sub-pages or sub-directories concerned on which the offending content is found, forthwith and in any event within 24 hours of receipt of a copy of the judgment alongwith requisite information from the Investigating Officer as directed below;

[28] 2021 SCC OnLine Del 1788

- A further direction was issued to the search engines to endeavour to use automated tools, to proactively identify and globally disable access to any content which is *exactly identical* to the offending content, that may appear on *any other websites/online platforms*;

- The Investigating Officer was directed to furnish in writing the Web URL and Image URL of the offending content to the other entities to whom directions have been issued by the court in the instant matter, alongwith a copy of the judgment, within 24 hours of receipt of such copy;

- The Delhi Police was directed to obtain from the pornographic website concerned and from the search engines Google Search, Yahoo Search, Microsoft Bing, DuckDuckGo (and any other search engines as may be possible) all information and associated records relating to the offending content such as the URL, account ID, handle name, Internal Protocol Address, hash value and other such information as may be necessary, for investigation in the FIR registered in the instant case, forthwith and in any event within 72 hours of receipt of a copy of the judgment, if not already done so;

- Furthermore, the petitioner was granted liberty to issue written communication to the Investigating Officer for removal/access disablement of the *same or similar* offending content appearing on *any other* website/online platform or search engine(s), *whether in the same or in different context*; with a corresponding direction to the Investigating Officer to notify such website/online platform or search engine(s) to comply with such request, immediately and in any event within 72 hours of receiving such written communication from the petitioner;

- Notwithstanding the disposal of the present petition by the instant order, if any website, online platform, search engine(s) or law enforcement agency has any doubt or grievance as regards compliance of any request made by petitioner as aforesaid, such entity shall be at liberty to approach the High Court to seek clarification in that behalf.

The Court made it clear that non-compliance with the foregoing directions would make the non-compliant party liable to forfeit the exemption, if any, available to it generally under Section 79(1) of the IT Act and as specified by Rule 7 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; and shall make such entity and its officers liable for action as mandated by Section 85 of the IT Act.

4.2 Right to be forgotten is the right of online victim

In *Subhranshu Rout v. State of Odisha*[29] accused committed forceful sexual intercourse with

[29] 2020 SCC OnLine Ori 878

the victim girl but has also deviously recorded the intimate sojourn and uploaded all the objectionable photos using the fake Facebook account in the name of victim girl, in order to further traumatize her. Hon'ble Orissa High Court observed that if the right to be forgotten is not recognized. In matters like the present one, any accused will surreptitiously outrage the modesty of the woman and misuse the same in the cyber space unhindered. With regard to the objectionable photos court stated that, *allowing such objectionable photos and videos to remain on a social media platform, without the consent of a woman, is a direct affront on a woman's modesty and, more importantly, her right to privacy. Court while adding to issue of the right of the victim stated that there is an unprecedented escalation of insensitive behaviour on the social media platforms and the victim like the present one could not get those photos deleted permanently from the server of such social media platforms like Facebook.* Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 recognized the need to protect the privacy of personal data, but failed to capture the issue of the "Right to be Forgotten". Right to be forgotten which refers to the ability of an individual to limit, delink, delete, or correct the disclosure of the personal information on the internet that is misleading, embarrassing, or irrelevant etc. as a statutory right in Personal Data Protection Bill, 2019.. Under Section 27, a data principal (an individual) has the right to prevent continuing disclosure of personal data by a data fiduciary. Court points out that the said Bill carves out the "right to be forgotten"**.**

4.3 *Directions to Police force for conducting proper investigation in cyber crime cases*

Taking note of rising cyber crimes along with lack of preparedness on part of the police force to deal with cyber crimes. Calcutta High Court in *Subhendu Nath v. State of W.B*,[30] issued certain directions to ensure that the investigation of crimes involving electronic evidence is conducted in a fair, impartial and effective manner.

- Proper training of members of police force in reception, preservation and analysis of electronic evidence.
- Only the officers who have been trained in accordance to the manner as stated above shall be involved in the investigation of crimes involving offences under IT Act and the offences in which electronic evidence plays a pre-dominant part.
- Every district shall have a cyber cell comprising of officers with specialised knowledge in the matter of dealing with electronic evidence in order to render assistance to local police.

[30] 2019 SCC OnLine Cal 242

- A standard operating procedure regarding preservation, collection, analysis and producing electronic evidence to be submitted by Director General of Police, West Bengal on the next date of hearing.
- Specialized forensic units to be set up in the State in order to facilitate examination and/or analysis of electronic evidence.

V. CONCLUSION AND SUGGESTIVE MEASURES

The COVID-19 pandemic has only generated greater momentum around the unaddressed issue of cyber violence which was still there before the outbreak of COVID-19.The root causes are not the virus or the resulting economic catastrophe, but rather a power and control imbalance. Inequality between men and women, discriminatory attitudes and beliefs, and gender stereotyping all contribute to this imbalance. [31]If we want to eradicate online violence against women we need to develop longer-term strategic approaches that tackle underlying causes. Violence against women, offline and online, must be acknowledged as a manifestation of systemic marginalization of women throughout society. Enhancing "the use of enabling technology, in particular information and communications technology, to promote the empowerment of women" requires the elimination of online violence against women. This imbalance stems from inequality between men and women, discriminatory attitudes and beliefs, gender stereotypes, social norms that tolerate and perpetuate violence and abuse, and societal structures that replicate inequality and discrimination.

5.1 Need for Collaborative Efforts

In order to prevent and combat the phenomenon of violence against women, it is required that there should be a better cooperation between law enforcement agencies and the civil society. With the aim of reducing the growing incidences of online abuse, holistic approach is necessary which would lead India towards prevention of such cases. It is quintessential to have law enforcement agencies and other NGO to work together in providing assistance to the victims of online harassment so that victims of violence can trust the state institutional mechanisms and perpetrators to be held responsible for crimes of this field. Furthermore, other online platforms should also improve their mechanism to report abuse by clarifying what would be treated as abuse, identify and respond to threats and abuse. Social media companies like twitter, facebook, instagram, must improve their mechanism to report abuses so that women are not

[31] Ohchr.org, https://www.ohchr.org/documents/issues/women/wrgs/onepagers/gender_stereotyping.pdf (last visited Nov 22, 2021)

abused and harassed while using them.[32]

5.2Technical augmentation:

There is a necessity for law enforcement agencies to improve their technical capabilities to combat the growing threat landscape which has arisen as a result of the evolution of creative cybercrime strategies. It is critical to expand their skills through innovative technical empowerment of their personnel. This might be done in collaboration with other countries that have made significant progress in this area. Doing this would help our personnel to identify gaps in the technical capabilities and undertake steps to overcome them. Further, it would act as an enabler in the long terms for creating in-house advanced technical capabilities, better administration, focused investigation and to shorten the investigation time period.

5.3 Cyber Safety Awareness

There is an urgent need for innovative and appealing cyber awareness campaigns women should be informed about the most recent cybercrime and cyber frauds and means to tackle them. They should be encouraged to report all incidents of cyber frauds, without the fear of being ridiculed or harassed.[33] This would result not only in protecting women but prevention of crimes to a larger extent. Some of basic digital security tips include:

- Creation of a strong password
- Have different passwords for different accounts
- Downloading of apps from authenticated platforms and use two-factor authentication
- Logging out of social media accounts
- Women should not use public WIFI for sharing sensitive information, like online bank details
- Use antivirus software and, if possible, use a virtual private network[34]

Now with the aid of online reporting tools like National cyber crime reporting portal it is convenient to report online harassment by the victims of online harassment. The portal which is specifically dedicated for reporting online incidence of violence against women. Culture of reporting should be encouraged, for which dissemination of awareness is needed. has to be

[32] Toxic Twitter - Human Rights Responsibilities Amnesty International, https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-7/ (last visited Sep 6, 2021)

[33]https://ficci.in/spdocument/22982/FICCI%20%20EY%20Report%20%20Confronting%20the%20New%20Age%20Cyber%20Criminal.pdf (last visited Nov 22, 2021)

[34]Assuring women's safety in the virtual world @businessline, https://www.thehindubusinessline.com/opinion/assuring-womens-safety-in-the-virtual-world/article30956278.ece (last visited Oct 30, 2021)

circulated Women should report cybercrimes incidences immediately. When women will start reporting incidences immediately the crime it will curb the abuser to commit such crimes.

The pandemic has brought more challenges and allowed perpetrators with additional opportunities to digitally harm women while staying at home. Its time to recognise that crimes of violence against women and girls are rapidly increasing. There is a need for constant evaluation of cyber laws and procedure because women face difficulties while seeking redressal due to lack of awareness. Cyber criminality is perhaps the deadliest epidemic spread over the world in the new millennium which needs to be addressed on priority basis so that we can make progress towards the egalitarian agenda of Sustainable Development Goals 2030. In order to attain this goal it is necessary to advance gender equality and eliminating violence against women in all forms and women safety even during times of crisis.

*****