Library Progress International *Print version ISSN 0970 1052*
Vol.44 No.3, Jul-Dec 2024: P. 27527-27535 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Justice In Digital Era: Analysing Legal And Systemic Challenges In Online Gender-Based Violence

[1]Dr. Sakshee Sharma, [2]Dr. Tauheed Alam*, [3]Ms. Aishwarya Vatsa

[1]Assistant Professor, UPES, Dehradun
[2]Assistant Professor, UPES, Dehradun
[3]Assistant Professor, UPES, Dehradun

How to cite this article: Sakshee Sharma, Tauheed Alam, Aishwarya Vatsa (2024) Justice In Digital Era: Analysing Legal And Systemic Challenges In Online Gender-Based Violence. *Library Progress International,* 44(3), 27527-27535

ABSTRACT
The proliferation of information and communication technology (ICT) has transformed societal interactions, but it has also facilitated the migration of patriarchal structures into the digital domain, manifesting as online gender-based violence (OGBV). This article critically examines judicial responses to OGBV in India, highlighting the interplay between legal provisions and systemic challenges. By exploring landmark cases such as *Suhas Katti* (2004) and *Ritu Kohli* (2001), the article underscores the judiciary's evolving role in addressing emerging cybercrimes, including cyberstalking, non-consensual image dissemination (NCII), and photo morphing. It critiques judicial and investigative inadequacies, such as outdated statutory frameworks and insufficient technical training for investigating officers, which undermine effective adjudication of OGBV cases. Additionally, it addresses the judiciary's struggle with entrenched patriarchal biases, evident in lower court verdicts that often overlook the continuum of online-offline harms. Notably, the article emphasizes the potential of recent judgments which advocate for victim-centric approaches, intermediary accountability, and technological interventions to combat NCIID. Despite strides in judicial awareness and proactive guidelines, the article identifies systemic gaps, including the absence of specialized laws for crimes like doxing, cyberbullying, and gendered hate speech. It calls for comprehensive legal reforms, enhanced investigative capabilities, and gender-sensitized adjudication to effectively address OGBV. The discussion highlights the urgent need to bridge the digital justice gap by aligning legal mechanisms with the realities of the digital era, ensuring women's rights are upheld in cyberspace.

KEYWORDS
Gender, Online, Violence, NCIID, Judiciary, Legislations

Introduction

With the ICT enabled and expediated transformation of public sphere, by creation of online spaces, many structures formerly found offline, have encroached these online spaces as well. (Mudgwa & Jones, 2020) One such example would be gender-based violence having its foundations on the structures of patriarchy and misogyny, which has proliferated into the cyberspace in the form of online gender-based violence (OGBV).

The judiciary has been an instrumental pillar in contouring of various Indian laws and rights enumerated in the Constitution, and their orders and judgments are the voice box that communicates the law to the public. It is indispensable, therefore, to investigate whether in these changed times of dominance of ICT, has the judiciary refashioned its approach towards the new crimes that have sprung up along with the new modalities of old crimes. Initiating with the significant judgment passed in the Suhas Katti case (Tamil Nadu v. Suhas Katti, 2004), the judiciary gave the first conviction under the IT Act, 2000. The case was concerned with sending of obscene messages by the accused, by misusing a married women's identity. However, during this time, the IT Act 2000 contained no provision dealing with cyberstalking or obscene messages. It was in Ritu Kohli Case (Manish

Kathuria v. Ritu Kohli, 2001), that this gap was first highlighted. This case brought to the forefront the severity of cyberstalking cases and was instrumental in bringing the amendment to the IT Act 2000. Manish Kathuria, the culprit of the case was arrested by the Delhi Police for stalking Ritu Kohli via the internet. He illegally used her name to chat on websites using obscene language, inviting people from various parts of India and abroad to make obscene calls to her residence phone number. In retrospect, this also is a classic example of doxing. However, in the absence of provisions relating to it, it was dealt under cyberstalking. Another issue that raised concerns was the absence of befitting provisions to sufficiently deal with the offence. The police registered the case under section 509 IPC. However, the section only refers to words, gestures or acts intended to insult the modesty of a woman. This section was found ill fitted in this case, as the offence happened over the internet, which had no mention in the provision. This was an alarm to the government regarding the lack of provisions dealing with cyberstalking. This led to the amendment of the IT Act 2000, which included section 66A, which however, was later declared unconstitutional (Shreya Singhal v. Union of India, 2015). In 2011, a Delhi University student was convicted of stalking and online harassment of a woman by creating her fake profiles on social networking sites and thus defaming her. After the victim rejected the marriage proposal, her nightmare began where she was constantly subjected to cyber harassment by the perpetrator. He even used her fake profiles to communicate with her friends and defame her. (Chauhan, n.d.) In another important case (State [Cyber Cell] v. Yogesh Pandurang Prabhu, 2009), the Metropolitan Magistrate court gave another conviction in a cyberstalking case. The accused Yogesh Prabhu was convicted to four months imprisonment for cyber stalking and harassing a colleague, after being rejected by her.

Since Suhas Katti, judiciary has dealt with many cases involving OGHV and has contributed proactively to help develop, effective laws in the field. However, much has advanced in the field of ICT, and there are certain important questions, in light of which, the judicial trend towards OGHV should be analysed. This may be achieved by critiquing the orders and judgments of the Courts in respect to the following questions:

a. Are the existing legal provisions adequate to protect women from OGHV?
b. Which legal provisions are used popularly while deciding these emerging offences?
c. How do courts handle cases of OGHV in the context of patriarchal norms and existing gendered stereotypes?
d. Do societal inequalities impact cases of OGHV in the eyes of the court?
e. What challenges emerge in front of the criminal justice system while dealing with cases of OGHV?
f. Are the roles and responsibilities of online intermediaries adequately developed in order to facilitate the process of adjudication of OGHV?

The following section will attempt to delve into the above questions and evaluate the judicial approach in addressing OGHV cases.

It is interesting to note that in a plethora of cases involving non-consensual intimate image dissemination (NCIID), examined in this research article, where the accused allegedly intimidated the victim using the threat of posting their obscene photographs/video graphs on the internet, while section 504-506 I.P.C relating to criminal intimidation were almost always invoked, section 66E was rarely even mentioned in the chargesheet (S. Latha v. The Commissioner of Police, Greater Chennai & Ors., 2020; Mahendra Prajapati v. State of U.P., 2010; Mushtaq Shah and Ors. v. State and Ors., 2019; Naseem v. State of Haryana, 2020; Gourav Narendra Singh v. The State of Maharashtra and Ors., 2022; Ajay Kumar v. State (NCT of Delhi), 2020).

In the combined case of *Ranjitha* v. *K. Lenin and ors*., *Aarthi Rao* v. *Ranjitha* and *Nithya Dharmananda* v. *Ranjitha* (Aarthi Rao v. Ranjitha, 2017; Nithya Dharmananda v. Ranjitha, 2017; Ranjitha v. K. Lenin and Ors., 2011), involving attempt to rape, morphing of photographs and extortion based on threats to make the photographs viral, it is unfortunate to see that the trial court as well as the high court, only limited their scope to sections of the IPC, none of which referred to violation of privacy. Despite several references made to the fact that the accused took photographs of the complainant with his mobile phones, morphed them with nude photographs of other actresses, and with the help of accused 3, extorted money using threat to make the said photographs viral, the high court failed to comment on the absence of section 66E or 67 A of the IT Actin the charges registered.

During the course of this research, a few cases were found, where certain provisions of the IT Act were charge-sheeted, however, the trial court failed to convict the perpetrators for the said offences even when the evidence of video recordings created in contravention of section 66 E of the IT act was presented to the court (Anbarasu and

Ors. v. The State of Tamil Nadu, 2023). In the case of *Gagandeep Singh and Ors*. v. *State of Haryana* (Gagandeep Singh and Ors. v. State of Haryana, 2013), an FIR was filed against the accused under sections 294, 506, 376, 120-B IPC and 67 (a,b,c) of IT Act. The accused had, with the help of his friend prepared an obscene video from the photographs of the victim that he took with his mobile phone during a marriage ceremony. Later he raped the victim by threatening to upload the videos on the internet. The CD containing the said video was also recovered and presented before the trial court. Yet, the Additional Sessions Judge convicted the accused only for offences under section 376 and 506 read with section 120-B IPC, and for the remaining offences under the IT Act they were acquitted. The perplexity of the case lies in the fact that despite the disclosure statement made by the accused based on which the CD with obscene videos was recovered, the trial court failed to find the accused guilty of the offence under section 67 (a, b, c) of the IT Act. Further, on appeal against the conviction, the High Court, while finding the testimony of the victim to be true beyond reasonable doubt, made no comment on the non-conviction of the accused for the offences under the IT Act. Rather the court declared "*I do not find any illegality or infirmity with the impugned judgement passed by the trial court. Rather it is based upon proper appraisal and appreciation of evidence and correct interpretation of law*". Any conclusive comment for the reasoning behind this apparent miscarriage of law on the part of the trial court and the High Court is currently not possible as the trial court's order has not been uploaded on the website. However, it is imperative to note here, that currently under the Indian law, no provision specifically addresses the act of morphing the pictures of an individual. It is only through excessive extension of certain provisions under IPC i.e., section 509 and IT Act i.e., section 67A, that the act can be made punishable. This can be viewed as a major lacuna which can severely obliterate the ends of justice, as such, the vague application of these provisions in cases of photo morphing can lead to greater discretion of the courts in deciding the matter.

Such mentioned cases are perfect examples to exhibit, that in most of the cases cited, online or cyber offences have led to/facilitated the commission of various offline offences like criminal intimidation, extortion, rape, defamation etc., yet the judiciary has turned a blind eye to the continuum formed by the online-offline offences. Chargesheets filed and judgments in in such cases (Pradeep M.P v. The State of Kerala and Ors., 2023), with no explicit mention of alleged offence under section 66 E or 67 A of the IT Act, are indicative of a general trend of focussing almost entirely on the offences of the physical realm, while being oblivious to the cyber-offence of non-consensual capturing of intimate images, both at the investigation stage and during the trial. The omission of charges under section 66 E of the IT Act can reasonably be also attributed to the inadequacy or rather reluctance of the investigating officers in recovery of the evidence relating to the alleged video clips and photographs. According to a statement given by a police official in Karnataka, the tedious co-ordination through MLATS/Letters Rogatory in marshalling digital evidence for cybercrimes, is one of the reasons why preference is often given to investigating "more serious cases, like terrorism" (Gurumurthy et al., 2019).

The exactitude of the conjecture, regarding the inadequacy of the investigating agencies can be substantiated from the admission of an IO in a case related to NCIID (Pradeep v. State of U.P., 2016). In this case involving alleged rape and uploading of obscene videos of the victim on YouTube the judge commented, " … *the room in which the obscene photographs were clicked was not visited by him. He did not bother to contact the family members or in-laws of the victim. He admitted that during the course of investigation, he neither visited the house of the victim nor the accused nor recorded any statement. He has also admitted that he did not bother to investigate on the point as to from which cybercafe the obscene videos were uploaded, although when any video has to be loaded on the internet a URL number has to be generated by which its link can be identified. This I.O. did not bother to find out, whose numbers were given on the facebook account and he also did not bother to know about the mobile number of the accused. He further did not think that it was his duty to find out about the SIM and memory card recovered from the accused because it was recovered by the previous I.O. …… Thus, the investigation as conducted by all the three Investigating Officers, is speaking volumes for itself*." The testimony cited above, if taken in representative capacity, draws attention to the current state of investigations, being conducted in cases involving cyber-crimes. Without any specialised training or special mandates to be followed during the investigation of cyber-crimes, owing to their unique and technical nature, investigating officers severely compromise their capability to produce credible evidence before the court (Kailash Chand v. The State of Himachal Pradesh, 2022).

In a comparatively recent judgment (Shibani Barik v. State of Odisha, 2020), the High Court made two perceptive comments on the efficacy of the provisions in the IT Act and the competency of the investigative machinery in

conducting efficient investigation in matters of cyber-crime. The court opined "*The appropriate Government has got the social responsibility to put some fair regulatory burden on those companies which are proliferating such applications. Though certain sections of the Information Technology Act in conjunction with other Acts in force, do have the teeth to bite such offenders especially Sections 66E, 67 and 67A, which stipulates punishment for violation of privacy, publication and circulation of what the Act calls "obscene" or "lascivious" content, but grossly insufficient. The Information Technology Act, 2000 does impose an obligation upon such companies to take down content and exercise due diligence before uploading any content, but India lacks a specialized law to address the crime like cyber bullying*." The statements regarding the lack of specialised law, competent to deal with the crime of cyberbullying, morphing, gendered hate speech, doxing etc., and the insufficiency of provisions of the IT Act, are a glaring reflection into the lacuna that the existing IT legal framework is handicapped with. Without specific laws regulating these relatively new crimes of technological origin, our existing statutory law can only do so much to provide loosely applicable patchwork of existing laws, with considerable loopholes, that make convictions under them quite difficult. In the same breath, the court commented "*Another grim scenario often comes the fore is the traditional approach of the investigative machinery while dealing with such type of offences. Most of our investigating officers are neither well trained nor do they understand the nuances of cybercrime. It is imperative that the personnel engaged in investigation need to be imparted periodical training so as to upgrade their skill to investigate this kind of techno-legal issues. Further, improvement in the cyber intelligence, cyber forensics and cyber prosecution training are long overdue to boost the hitherto rickety cyber policing.*"

In a case involving online harassment and abuse of a female social activist, for including certain references of a young leader in her book, the high court made certain important observations in its order. The messages liked, tagged, and posted by the accused on his social media, had 'overtones of the subject raping young men, immorality, masturbation and promiscuous sexual behaviour'. Referring to cyber bullying, cybersexism and cyber misogyny, the court opined that the complainant has been subjected to discriminatory and abusive behaviour due to her political leaning and denied the accused anticipatory bail. While commenting on the potential of using social media to disparage the reputation of an individual the court commented "*In the virtual world of social media, people feel that they are free to send insulting or abusive messages to others. Though the strength of social media has always been to easily connect and interact with friends and groups, it can also be subjected to gross abuse. The freedom that social media offers cannot be exploited to do online baiting such as in the instant case wherein the de facto complainant is branded as being sexually promiscuous*" (Majeesh K. Mathew v. State of Kerala and Ors., 2018).

Bail petition in the case of (Naseem v. State of Haryana, 2020), not unlike others revolves around the facts that the prosecutrix, a minor was repeatedly raped by the petitioner and his friends by threatening her to make the video of her rape at the first incident viral. She was even threatened not to relate the incident to anyone or else her entire family will be shamed in the village owing to the video that will be made public. Since this was a bail petition, the trail court had not decided the case on its merit. However, for the purpose of this study, the order of the High Court allowing the bail petition and the rationale forwarded for the same, is of interest. The court while making the order made certain observations which align with the premise that the judiciary needs to adopt a sensitised approach towards gender-based crimes. It is suggested that the court in the verdict was remiss in commenting that, since the fact that the prosecutrix was a married girl, was not disclosed at the time of filing of FIR by the complainant (her father), and that there was an inordinate delay of five months in reporting the matter to the police, it creates a serious doubt on the reliability of the statement of the complainant. The court while giving the above-mentioned rationale, seem to have contradicted the view of the Supreme Court in (State of Punjab v. Gurmit Singh & Ors., 1996) and (Deepak v. State of Haryana, 2015), where the court opined "*the Courts cannot overlook the fact that in sexual offences and in particular, the offence of rape and that too on a young illiterate girl, the delay in lodging the FIR can occur due to various reasons. One of the reasons is the reluctance of the prosecutrix or her family members to go to the police station and to make a complaint about the incident, which concerns the reputation of the prosecutrix and the honour of the entire family*" (Deepak v. State of Haryana, 2015).

It is essential to note that such statements by the court which judicially stereotype women are greatly divergent from the guidelines issued for the courts by the Supreme Court in (Aparna Bhat v. State of Madhya Pradesh, 2021) that while dealing with sexual crimes, *"...Bail conditions and orders should avoid reflecting stereotypical or*

patriarchal notions about women and their place in society, and must strictly be in accordance with the requirements of the Cr. PC. In other words, discussion about the dress, behaviour, or past "conduct" or "morals" of the prosecutrix, should not enter the verdict granting bail", and *"Judges especially should not use any words, spoken or written, that would undermine or shake the confidence of the survivor in the fairness or impartiality of the court"*. It is unfortunate that the Apex court needs to spell out and remind these foundational principles to the judicial officers, who are ideally expected to be immune to the urge, of letting their personal and stereotypical biases impact their judgments. However, when verdicts of the courts are plagued with statements like "*I am aware of the fact that a woman, howsoever dissolute, she may be, would not ordinarily consent to insulting, humiliating and repulsive act of sexual intercourse on her. Law recognises that a woman even of easy virtue or even a whore for that matter has personal dignity and owner"* (Pradeep v. State of U.P., 2016) and *"she has also not objected to consuming drinks with the petitioner and allowing him to stay with her till morning; the explanation offered by the complainant that after the perpetration of the act she was tired and fell asleep, is unbecoming of an Indian woman; that is not the way our women react when they are ravished"* (Sri Rakesh B v. State of Karnataka, 2020), it is only judicious on the part of the Apex Court to admonish the lower courts when they strengthen the sexist and misogynistic norms of the patriarchal society through their verdicts.

If we consider the statutory provisions majorly observed to be evoked in the cases involving various forms of OGBV generally and NCIID specifically, like section 66E of the IT Act, section 509 of the IPC, and section 354 C of the IPC, what is striking is the limited scope of privacy within which these provisions operate. The references to the 'body' or 'private area' or 'modesty' of the women in the text of the provisions, delimits the essence of privacy only in the context of a woman's body and circumvents women's agency. The Victorian reference of 'Outraging the modesty of a woman', found in section 354 and section 509 of the IPC, finds its roots in the patriarchal stereotypes of woman's worth being determined by her modesty. Even in cases where the courts aim to adopt a victim-centric approach that avoids moral judgments or shaming, the legal 'protection' extended to women often runs counter to feminist movements, as it perpetuates patriarchal ideals like honour, modesty, and virtue attributed to women. Such narrow reference to privacy, not only alienate it from its wider fundamental right jurisprudence, but also reinforces the tropes of women's right to privacy deriving legitimacy primarily for the protection of her modesty and not her agency (Rupan Deol Bajaj v. Kanwar Pal Singh Gill, 1995; State of Punjab v. Major Singh, 1967; Raju Pandurang Mahale v. State of Maharashtra, 2004)

One important issue related to consent in cases of NCIID arises when the intimate image is captured with the consent of the, but is disseminated without caring to get her consent, or where the initial consent for such dissemination has been withdrawn. In an important case of (X v. Youtube, 2013) the High Court of Delhi delved into the abovementioned issue. Additionally, the case also revolved around another important question of whether right to be forgotten can be considered as a statutory right. The plaintiff had submitted her demonstration videos containing explicit scenes of nudity to the producer of a film. Later, even though the project got shelved, the demonstration videos were uploaded by the producer without her consent. Upon her request, the producer deleted the video, however, it kept resurfacing on various websites including YouTube. The plaintiff approached the court seeking interim protection and a takedown of the video claiming it to be a violation of her privacy on account of the damage to her reputation and the harassment faced by her. Additionally, she claimed her right to be forgotten too is being violated owing to the defendant's failure to prevent republication of the videos. The defendants (websites, internet service providers and search engines) relied on (Karthick Theodre v. Registrar General, 2021) and (Subhranshu Rout v. State of Odisha, 2020) and argued that they did not have any obligation towards the petitioner for the prevention of the republication of the concerned videos as there exists no statutory law regarding right to be forgotten. The defendants amongst other arguments, also asserted that since the plaintiff filmed the videos consensually, she cannot rely upon either right to be forgotten, or Rule 3(2)(b) of the IT Rules 2021.

While the Court acknowledged that the case involves questions that need an extensive consideration, it rejected the arguments of the defendants that consent on the part of the plaintiff to be filmed barred her from taking legal recourse for the removal of the content from the internet. The Court found that the consent of the plaintiff has since been expressly withdrawn through her request to the producer to take down the content from his channel. Quoting (Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd., 2019) the Court stated that owing to the explicit nature of the content, and the impact it may have on the reputation, it is only prudent to protect the right to privacy. Regarding the 'right to be left alone' and 'right to be forgotten', the court addressed the question in somewhat ambiguous terms. Refusing to give a final conclusion on the matter, and acknowledging that the Hight

Courts of Madras and Orissa have not recognised right to be forgotten as a statutory right, the Court relied upon the decision in (Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd., 2019) and opined that the plaintiff is entitled "to be left alone" and "to be forgotten".

States have a direct responsibility concerning violence perpetrated by agents of the State itself. They also have due diligence obligations to prevent, investigate and punish acts of violence against women committed by private companies, such as Internet intermediaries, in accordance with article 2 (e) of the Convention on the Elimination of All Forms of Discrimination against Women. According to article 4 (c) of the Declaration on the Elimination of Violence against Women, States should exercise due diligence to prevent, investigate and punish acts of violence against women. (U.N. Human Rights Council, 2018, p. 62)

In a recent judgment by the High Court of Delhi in (X v. Union of India, 2023, para. 39), a case concerning the distressing situation of a woman whose intimate photos were posted on pornographic websites without her consent, made some important strides towards evolving a mechanism for providing expeditious relief to the victims of NCII and also to alleviate their trauma. The petition claimed that a YouTube channel was created in the petitioner's name and was used as a platform to upload her explicit videos and photographs daily. The petitioner stated that despite approaching the Grievance Cells of Google LLC, Microsoft India Pvt. Ltd., YouTube.com and Vimeo.Com, and filing numerous complaints on cybercrime.gov.in,the petitioner received no relief in the form of taking down of the explicit photos, as they kept on resurfacing again even after their deletion. Before diving into the analysis of the arguments produced by the respondents, the court pointed out that the ubiquitous nature of the internet facilitates faster and easier dissemination of any unlawful content, while the speed of the content dissemination makes it exceptionally difficult to remove such content from the internet permanently. Thus, in cases of NCIID, promptness of action is required on the part of the stakeholders to ensure, that the victim doesnot have to undergo repeated distress everytime the content resurfaces on some different platform or site (X v. Union of India, 2023, para. 39). The court while siting the judgment in *K.S. Puttaswamy* case observed that uploading of NCII apart from being a direct violation of the provisions of the IT Act and the IT rules, also results into a grave violation of the right to privacy of the victim. It is the right to privacy which grants individuals decisional and informational autonomy, thus empowering them to exercise control over information pertaining to them. In response to the contention of the Respondents, that as search engines do not host or publish or create content themselves, and do not have any control over any content, as it merely indexes the content by third-party on their websites/platforms, the court asserted that the search engines undeniably do have the ' ability, the capacity, and the legal obligation to disable access to the offending content.' The court also remarked on the exhibition of a lackadaisical attitude by the intermediaries and the state in providing relief to the trauma-stricken victim, while vehemently advancing arguments to shirk off their responsibilities and blameworthiness. After a detailed analysis of the arguments advanced by the parties, the court deemed it fitting to pronounce certain directions to the respondents, in order to ascertain prompt and efficient remedying of a victim's distress. The directions included the following:

1. Petitioners seeking content takedowns related to NCIID must submit a sealed affidavit identifying specific problematic audio, visual content, keywords, and URLs, along with their petitions, to ensure swift assessment of their legality.
2. The definition of NCII should be interpreted liberally to include any sexual content acquired without consent and in violation of an individual's privacy. The Intermediaries must also ensure that their designated Grievance Officers are sensitized to handle complaints related to NCIID.
3. The 'Online Cybercrime Reporting Portal' should feature a status tracker for complainants, offering updates from filing a complaint for content removal. It must also display redressal mechanisms accessible to victims in multiple languages.
4. Upon receiving information about NCII content punishable under Section 66E of the IT Act, the Delhi Police must promptly register a formal complaint to initiate an investigation and apprehend perpetrators swiftly, preventing further unlawful content uploads.
5. Each district cyber police station must designate an officer to liaise with intermediaries, facilitating the resolution of grievances within specified timeframes as per IT Rules.

6. Establish a 24/7 helpline for reporting NCII content. Operators must be trained to handle NCII issues sensitively and should not engage in victim-blaming. They should have access to a database of counsellors and psychologists for victim support.
7. Search engines must employ hash-matching technology (Ofcom, 2022, p. 3) to identify and remove NCII content promptly. The claim that they lack such technology is not acceptable.
8. Intermediaries should prominently display the reporting mechanism under Rule 3(2)(c) of the IT Rules on their websites, ensuring users are aware of the process.
9. the specified timeframes under Rule 3 of the IT Rules should be followed rigorously. Deviations may result in the search engine losing liability protection.
10. Search engines should adopt a token or digital identifier-based system when victims obtain takedown orders. It the same content resurfaces, search engines must use existing tools to prevent access, sparing victims from repeated legal processes.
11. Consider developing a secure their-party encrypted platform in collaboration with search engines under Rule3(2)(c) for registering and automatically removing offending NCII content, reducing the burden on victims.

The judgment holds significance as, firstly, it tends to move beyond the concept of physical privacy in cases of OGHV and discusses informational and decisional privacy quite substantially. Thus, opening the doors for a broader interpretation of privacy to be taken into consideration while dealing with such instances. Secondly, the directions and recommendations provided by the court aim to streamline the process of addressing NCIID cases by providing timely relief to victims while holding intermediaries accountable. The implementation of these guidelines is expected to significantly improve the resolution of OGBV issues in the long term. It introduces a proactive and efficient approach to handling such cases, reducing the trauma faced by victims and ensuring that perpetrators are swiftly brought to justice. The emphasis on user awareness, intermediary accountability, and advanced technological solutions should enhance the overall effectiveness of combatting cyber-harassment against women. Additionally, the establishment of a round-the-clock helpline and access to mental health support signifies a holistic approach to addressing the mental health concerns of the victims.

Conclusion

The judicial response to Online Gender-Based Violence (OGBV) in India reveals both commendable strides and persistent challenges. As this research underscores, while courts have taken steps to address emerging cybercrimes, systemic gaps in legal frameworks and investigative capabilities hinder comprehensive justice. On critical analysis of the disconcerting trend within the lower courts reveals the predilection for prioritising offline crimes over their online counterparts., reflecting an incomplete understanding of the evolving nature of such crimes. This underscores a systematic gap that exists, which inadequately acknowledges the continuum of harm experienced by victims. However, by acknowledging the disconcertment of inadequacies in existing legal frameworks and the dearth of specialised investigating officers, the judiciary has acted as a vanguard of justice in the digital age.

Encouragingly, landmark judgments have emphasized the need for enhanced accountability from intermediaries and advanced remedies for victims. However, outdated legal provisions, insufficient training of investigative officers, and a reluctance to adapt traditional legal tools to digital realities often impede the timely and effective adjudication of cyber-related cases. Moreover, patriarchal biases and stereotypical notions about women's behavior continue to influence judicial outcomes, countering the principles of victim-centric justice.

To ensure justice aligns with the realities of the digital age, reforms are necessary. These include updating laws to encompass specific acts like morphing, doxing, and gendered hate speech; sensitizing judiciary and law enforcement; and fostering a holistic legal framework that respects women's autonomy and privacy. By addressing these gaps, the judicial system can better protect against OGBV, ensuring it empowers rather than undermines women's rights in the digital era.

References

[1] Mudgwa, C., & Jones, K. (2020, April 9), As use of digital platforms surges, we'll need stronger global efforts to protect human rights online. The Conversation. Retrieved from https://theconversation.com/as-use-of-digital-platforms-surgeswell-need-stronger-global-efforts-to-protect-human-rights-online-135678

[2] Tamil Nadu v. Suhas Katti. (2004), *Case No. 4680 of 2004*
[3] Manish Kathuria v. Ritu Kohli, *Criminal Case No.* 14616/2014.
[4] Shreya Singhal v. Union of India. (2015), *All India Reporter*, SC, 1523
[5] Chauhan, N. (n.d.). DU law student charged with cyber stalking. *Times of India*. Retrieved from https://timesofindia.indiatimes.com/city/delhi/du-law-student-charged-with-cyber-stalking/articleshow/8917937.cms
[6] State (Cyber Cell) v. Yogesh Pandurang Prabhu, (2009). *Criminal Case No. 3700686/PS/2009*
[7] Aarthi Rao v. Ranjitha, Criminal Petition Nos. 6009 of 2017, [2017] 8 *Supreme Court Cases* 210
[8] Ranjitha v. K. Lenin and Ors., Criminal Revision Petition No. 763 of 2011, [2011] 11 *Supreme Court Cases* 305
[9] Aarthi Rao v. Ranjitha, Criminal Petition Nos. 6009 of 2017, [2017] 8 *Supreme Court Cases* 210
[10] Nithya Dharmananda v. Ranjitha, Criminal Petition Nos. 6010 of 2017, [2017] 8 *Supreme Court Cases* 215
[11] S. Latha v. The Commissioner of Police, Greater Chennai & Ors. (2020). *Habeas Corpus Petition No. 293 of 2020*
[12] Mahendra Prajapati v. State of U.P., Criminal Appeal No. 7451 of 2010, [2010] 10 *Supreme Court Cases* 451
[13] Mushtaq Shah and Ors. v. State and Ors., (2019) 3 *Jammu and Kashmir Judicial Reports* 372
[14] Naseem v. State of Haryana, (2020) 3 *Reporter of Criminal Judgments (Criminal)* 527
[15] Gourav Narendra Singh v. The State of Maharashtra and Ors., (2022) *All Maharashtra Reports (Criminal)* 916
[16] Ajay Kumar v. State (NCT of Delhi), (2020) 3 *Supreme Court Cases* 512
[17] Anbarasu and Ors. v. The State of Tamil Nadu, (2023) *Manupatra*/TN/1214/2023
[18] Gagandeep Singh and Ors. v. State of Haryana, (2013) *Manupatra*/HR/3845/2013 and 3846/2013
[19] Pradeep M.P v. The State of Kerala and Ors., (2023) *Criminal Law Journal* 401
[20] Gurumurthy, A., et al. (2019). Born digital, born free?: A socio-legal study on young women's experience of online violence in South India. *IT for Change*. Retrieved from https://itforchange.net/index.php/born-digital-born-free-a-socio-legal-study-on-young-womens-experiences-of-cyberviolence-south-india
[21] Pradeep v. State of U.P., (2016) 2 *Allahabad Criminal Reports* 1377
[22] Pradeep M.P v. The State of Kerala and Ors., (2023). *Criminal Law Journal*, 401.
[23] Gurumurthy, A., et al. (2019). *Born digital, born free? A socio-legal study on young women's experience of online violence in South India*. IT for Change. Retrieved from https://itforchange.net/index.php/born-digital-born-free-a-socio-legal-study-on-young-womens-experiences-of-cyberviolence-south-india
[24] Pradeep v. State of U.P., (2016). *Allahabad Criminal Reports*, 2, 1377.
[25] Kailash Chand v. The State of Himachal Pradesh, (2022). *Manupatra Judgments*. M.A.N.U./H.P./0486/2022.
[26] Shibani Barik v. State of Odisha. (2020), *All India Cases*, 212, 871
[27] Majeesh K. Mathew v. State of Kerala and Ors., (2018). *Kerala Law Reports*, 3, 583
[28] Naseem v. State of Haryana, (2020). *Recent Criminal Reports (Criminal)*, 3, 527
[29] State of Punjab v. Gurmit Singh & Ors., (1996). *Supreme Court Cases*, 2, 384
[30] Deepak v. State of Haryana. (2015), *Supreme Court Cases*, 4, 762
[31] Aparna Bhat v. State of Madhya Pradesh, (2021). *Supreme Court Cases Online*, S.C.C. OnLine S.C. 230
[32] Pradeep v. State of U.P., (2016). *Allahabad Criminal Reports*, 2, 1377
[33] Sri Rakesh B v. State of Karnataka, (2020). *Criminal Petition No. 2427*
[34] Rupan Deol Bajaj v. Kanwar Pal Singh Gill, (1995). *Supreme Court Cases*, 6, 194
[35] State of Punjab v. Major Singh, (1967). *All India Reporter*, 63

[36] Raju Pandurang Mahale v. State of Maharashtra, (2004). *Supreme Court Reports*, 2, 287
[37] Subhranshu Rout v. State of Orissa, (2020). Bail Application No. 4592
[38] Smt Qamar v. State of Telangana, (2021). Bail Application No. 3669
[39] Guruvinder Singh v. State of Uttar Pradesh, (2021). Bail Application No. 3430
[40] Subhranshu Rout v. State of Odisha, (2020). Supreme Court Cases Online Orissa, Ori 878
[41] Karthick Theodre v. Registrar General, (2021). Supreme Court Cases Online Madras, Mad. 2755
[42] X v. YouTube, (2013). Criminal Appeal No. 14/2013
[43] Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd. (2019). Supreme Court Cases Online Delhi, Del. 8494
[44] U.N. Human Rights Council, (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective (A/HRC/38/47, p. 62)
[45] X v. Union of India, (2023). Delhi High Court, DHC/002806, para. 39
[46] X v. Union of India, (2023). Delhi High Court Cases, DHC/002806, para. 39
[47] Ofcom. (2022). Overview of perceptual hashing technology (p. 3) https://www.ofcom.org.uk/__data/assets/pdf_file/0036/247977/Perceptual-hashing-technology.pdf