INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

VIOLENCE AGAINST WOMEN IN INDIA ON THE INTERNET: SOCIO-LEGAL ANALYSIS OF ONLINE VIOLENCE WITH REFERENCE TO MADHYA PRADESH

AUTHORED BY - MS. GEENY MOURYA,
Research Scholar,
Institute of Legal Studies and Research, Mangalayatan University, Aligarh, U.P.

CO-AUTHOR - DR. HAIDAR ALI,
Associate Professor,
Institute of legal Studies and Research, Mangalayatan University, Aligarh, U.P.

ABSTRACT

The internet today has turned out to be a potent communication, connectivity and interaction medium in the digital era of communication. Nevertheless, media are the ones that provided voices with the means of being used as means of violence, abuse, and intentional violence. Online violence has no geographical or time boundaries which have caused intense psychological and social damages on the victims. However, this article does not just represent online violence as a technical/personal problem, but as a complicated social and legal phenomenon, which has the reflection of inequalities and discrimination in the general. By means of critical reflection of different forms of digital abuse, i.e. cyberstalking, trolling, image-based abuse, and hate speech, the study considers whether the existing legal provisions, both on international and national levels, are sufficient to combat the harms. It also discusses the role of online intermediaries and social media websites in the formulation of online behaviors and responsibility. Finally, the paper will deal with legal and judicial background of cybercrime, focusing on state of Madhya Pradesh then suggest a more unifying way out of the issue which is the combination of law, technology and social education to ensure dignity, safety and rights on the internet world.

Keywords: Online Violence; Cyber bullying; Gender-based violence; Information Technology Act, 2000.

ISSN: 2582-6433

Introduction

The mind bending digitalization of the contemporary society has altered the way people interact, mingle and exercise their expression. The internet and social media outlets have been the indomitable tools of empowerment in which voices that never had a platform to be heard in the society had a platform to express themselves. However, it is the same digital revolution, which has brought new fissures.[1] What used to be few occurrences of cyber aggression has now become a tawed social group of phenomena, called online violence; a kind of harm inflicted online, but with extremely tangible and long-term effects. A subset of these crimes, largely facilitated by the anonymity and speed of virtual networks, online violence, is likely to erase the distinction between civic and personal harm. Social impact is extreme, that is, psychological trauma, reputation, professional and social isolation. Such behavior (according to the law) challenges the nature of traditional crime, evidence, and jurisdiction at the international level compelling legal systems all over the world rethink how justice operates within the digital space.[2]

The Information Technology Act, 2000 (IT Act) is the main Act or legislation that is used in controlling the behavior of the cyberspace within the Indian context. This was originally designed to enable e-commerce and electronic governance but today it has been extended to incorporate online crime. The provisions like the Section 66C (identity theft), Section 66D (cheating by personation using computer facilities), Section 67 and 67A (obscene material and sexually explicit material), and Section 69A (blocking the access of information to the public) are trying to restrain the various kinds of virtual wrongdoing. However, the limitations of the Act have been challenged time and again, most famously in Shreya Singhal v. Union of India (2015), where the Supreme Court ruled that Section 66A was unconstitutional on the counts of vagueness and infringing free speech under Article 19(1)(a). What was so crucial in this landmark ruling was to caution of the precariousness of a line of thinking between ensuring citizens are not harassed by use of the Internet and preserving the value of freedom-of-speech in an online democratic sphere.[3]

[1] *Intermediary Liability*, CONSTITUTIONAL LAW AND PHILOSOPHY, https://indconlawphil.wordpress.com/tag/intermediary-liability/. (last visited Oct. 8, 2025).
[2] *Uniting for Global Cyber Resilience | CyberPeace*, https://www.cyberpeace.org (last visited Oct. 8, 2025).
[3] *The Judiciary's Tryst with Online Gender-Based Violence: An Empirical Analysis of Indian Cases and Prevalent Judicial Attitudes | IT for Change*, https://itforchange.net/judiciarys-tryst-online-gender-based-violence-an-empirical-analysis-of-indian-cases-and-prevalent (last visited Oct. 8, 2025).

ISSN: 2582-6433

The IT Act is not the only law, the provision of the Bharatiya Nyaya Sanhita (BNS) is also applied on online violence. Section 78 (stalking), Section 356 (defamation), Section 351(4) (criminal intimidation by anonymous communication) and Section 79 (word, gesture or act intended to offend the modesty of woman) are some of the examples that are being quoted at an increasing rate in cyber cases. The judicial explanations of such provisions have expanded to cover cyber harassment and cyber intimidation. Nevertheless, due to the presence of numerous laws and multiple jurisdictions, the issue of procedural ambiguity and lack of enforcement tends to arise, and the victim is left with little or nothing to retrieve.

The solutions to online violence at the international level have common issues. The most important international cyber treaty that persists in aligning the laws of cybercrime and enhance the cooperation across the states is the Budapest Convention on Cybercrime (2001). In the meantime, the UN Human Rights Council, and UN Women have already established that online gender-based violence is a type of violence that violates human rights and, therefore, member states should aim to provide comprehensive protection against it online.[4] The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) General Recommendation No. 35 (2017) also emphasizes the reality that the issue of gender-based violence has now been applied to technological spheres. These instruments together confirm that the digital world is not out of reach for human rights law.[5]

Socially, cyber violence is a recreation of the discrimination and power patterns in the society. Women, the LGBTQIA+ and other minority groups receive a disproportionate number of attacks on the internet. Organizations such as the Amnesty International and UNESCO surveys have shown that the women journalists, activists and even the people in the limelight are more prone to targets, usually in the name of sexual violence or even character defamation. Such abuse has become a part of the society under the pretext of free speech or internet banter that has led to the culture of silence and impunity. This digital design in conjunction with the social inequality causes the online spaces to appear as the extensions of the offline patriarchy and prejudice.[6]

[4] *Technology-Facilitated Gender-Based Violence: A Growing Threat | United Nations Population Fund*, https://www.unfpa.org/TFGBV (last visited Oct. 8, 2025).
[5] *General Recommendation No. 35 (2017) on Gender-Based Violence against Women, Updating General Recommendation No. 19 (1992) | OHCHR*, https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-35-2017-gender-based (last visited Oct. 8, 2025).
[6] *Safety of Women Journalists | UNESCO*, https://www.unesco.org/en/safety-journalists/safety-women-journalists (last visited Oct. 8, 2025).

ISSN: 2582-6433

The other important point of interest is the role played by social media websites in intermediate and regulation of the content. These are now referred to as Twitter (formerly called X) Instagram, Facebook, YouTube, and other sites are said to be online intermediaries, as stipulated in Section 79 of the IT Act and the sites are granted partial immunity to cause harm in case they exercise reasonable care to do so. In an effort to hold the intermediaries responsible, digital media ethics code, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, implemented by the Government of India provides conditions of grievance redress and traceability requirements. Nevertheless, a question still remains on whether the chilling of free speech and the capability of algorithmic-based content moderation instruments to do so in order to capture more nuanced abuse, like coded hate speech or targeted disinformation.[7]

The issue then is to offer a social and legal system that will simply respond to internet violence without infringing upon the rights of the internet. This malice cannot be chased away by law but should be backed up by awareness, digital literacy and responsible design of technologies. It is a regulation issue as it is also an institutional responsiveness and culture change one.[8]

The paper examines these dynamics in a dual manner, i.e. social (with special focus on trends, perceptions and effects of online violence) and legal (the review of statutory law, judicial response and policy failure). Moreover, the paper will present an argument that, despite the fact that online violence mediator is technology, it is, still, a social phenomenon, which should be treated as the interconnected one in the approach of rights. The second sections talk about the nature and type of violence on the Internet, how effectively legal measures will be sufficient to the problem in India, the role of digital intermediaries. The third section deals with the legal framework and judicial development of cybercrime in India. Further, the paper deals with the cybercrime in the state of Madhya Pradesh. Finally, the paper concludes and suggest what reforms may be needed to make online spaces safer and more accommodative.

[7] *Press Release: Press Information Bureau*, https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1700749 (last visited Oct. 8, 2025).
[8] *(PDF) Combining Parental Controls and Educational Programs to Enhance Child Safety Online Effectively*, https://www.researchgate.net/publication/384301419_Combining_parental_controls_and_educational_programs_to_enhance_child_safety_online_effectively (last visited Oct. 8, 2025).

ISSN: 2582-6433

Nature and Forms of Online Violence

As the internet as the major communication media is now taking root, it has changed permanently the way people interact and communicate, and define identity. But has also created new means of violence that discontinues physical space.[9] Violence in the form of any form of aggression, harassment, or harm committed using digital technologies has become an unpleasant aspect of contemporary social life. Even though dedicated in the virtual world, the psychological, reputational and emotional fallout transfers to the physical one, destroying the old paradigm of online and offline violence.[10]

The difference between the online and traditional violence lies in the fact that the former is more anonymous, enduring and broad. Internet helps criminals to live anonymously, escape the repercussions and disseminate damaging information to masses at the same time. It is also worsened by the reality that digital footprint, messages, videos, or pictures cannot be easily deleted or regulated by the victims thus they cannot eliminate any scathing texts.[11] Secondly, the transferability of the digital content in question will ensure that in case of abuse, that very content can be re-lived in some form of repetitions through sharing, reposting, or taking screenshots.

The definition of online or technology-enabled violence by the United Nations General Assembly defines it as any violence which is perpetrated, enabled, or even condoned in any manner, through the use of information and communication technologies (ICTs), whether of a gender based nature. This definition asserts that, online violence is not a phenomenon per se, but is an extension of social and gender systems that have been transferred to the virtual world.[12]

The range of violence in cyber world is diverse and it keeps changing with the changing technology. Social or practical definition of cyberstalking Cyanoscopic and unwanted monitoring or peeking into the online activity of an individual is covered in the scope of the practice of cyberstalking, in most cases with threatening or threatening messages. Section 78

[9] *Ibid.*
[10] *India: Shielding Your Privacy in the Age of Intelligent Systems - HG.Org*, https://www.hg.org/legal-articles/india-shielding-your-privacy-in-the-age-of-intelligent-systems-68650 (last visited Oct. 8, 2025).
[11] *How Has Social Media Emerged as a Powerful Communication Medium?*, https://www.ucanwest.ca/blog/media-communication/how-has-social-media-emerged-as-a-powerful-communication-medium (last visited Oct. 8, 2025).
[12] *Ibid.*

ISSN: 2582-6433

of the Bharatiya Nyaya Sanhita is a criminal act of cyberstalking. The term cyberbullying is defined as hate speech, intimidation, or humiliation against individuals and more so, children and young adults via the use of the internet or digital media.[13] Psychological effects of depression, anxiety and self-harm also have been attributed to cyberbullying which lends it significance in the health of the population.

Image-based sexual abuse (IBSA) is a type of production, distribution, or sharing of intimate images without permission, and most frequently as a manipulation method or a humiliation strategy. In Information Technology Act of 2000, section 67 and 67A covers the problem of obscene and sexually explicit material on the Internet that is published. Doxing may be defined as the sharing of personal or identifying information in open forums without consent and may spark the physical danger of harm or harassment to the victim. Internet hate speech involves the spread of discriminative, derogatory, or violent information about people or groups of people on the basis of their race, religion, gender, and identity. Though to a certain degree handled within the provisions of 196, 299 and 353 of the Bharatiya Nyaya Sanhita, the digital version of these disseminations is highly hard to prosecutes as the medium is offered online.[14]

Troll and Internet harassment is an intentional act of provocation or sustained abusive behavior to upset, or threaten the people especially those who have a dissenting or minority of opinion. Deepfakes and impersonation are a type of fraudulent use of personal data or AI-generated fake images, audio, or video that cause damage to reputation and agreement. The response of deepfakes is yet to be found in the laws, yet they pose critical issues over privacy in the Articles 21 of the Indian Constitution.[15]

Online violence affects communities and women who are in a marginalized position more. As it has been discovered, women, especially young women are more likely to fall victim to sexual abuse and threats via the internet. In India, the Amnesty International located a research on the misuse of social media, the results of which showed that a significant

[13] General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992) | OHCHR.
[14] *Does the Internet Bring People Closer Together or Further Apart? The Impact of Internet Usage on Interpersonal Communications - PMC*, https://pmc.ncbi.nlm.nih.gov/articles/PMC9687672/ (last visited Oct. 8, 2025).
[15] *Ibid.*

ISSN: 2582-6433

percentage of the abuse involves women politicians and activists. Through such gendered targeting, there is a recreation of the patriarchal domination, where they are trying to hush down the women in the daily discourse. What makes the matter even more intricate is the intersectionality: individuals belonging to oppressed castes, ethnicities, religious minorities and LGBTQIA+ are likely to be the victims of several, overlapping kinds of online harm that only increase the corresponding imbalance of the social circumstances in the real life.[16]

Besides identity and gender, there exists also desperate psychological, social and economical effects of online violence. It results in anxiety, depression and post-traumatic stress among the victims. This mistreatment can be extended to the working and academic life and restrict the opportunities and chances to interact with the people. The structural character of the harms depicts the fact that cyberbullying is not an isolated issue of technical or individual problem, but an issue of the society and law that should be addressed on multi-dimensional levels.[17]

Legal Framework and Judicial Approaches

The creation of cyber communication in a short time span also put a strain on the legal systems established by tradition to keep pace with the number of variants of the web-based violence that appeared daily. Even though in virtual world, cyber violence is a violation to some of the basic human rights including right to privacy, right to equality and right to dignity in the Indian Constitution. Therefore, there must be statutory law, and the interpretation of law by the judiciary in the definition, regulation and limitation of such behavior.[18]

The main legislation in India that bears reference to cyber misconduct is the Information Technology Act, 2000 (IT Act). The IT act was put in place primarily with the aim of supporting electronic governance and e-commerce, it has been changed to incorporate crimes of a digital harassment and cybercrime. Personation cheating and identity theft by the use of computer resources is an offense in section 66C and 66D. Part 67 and 67A refers to the issuance and dissemination of obscene and sexually explicit contents including the image based sexual abuse. Part 69A gives the government authority to subvert access to the harmful information

[16] *Digital Violence Against Women: Is There a Real Need for Special Criminalization? | International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, https://link.springer.com/article/10.1007/s11196-024-10179-3 (last visited Oct. 8, 2025).
[17] *Cyberbullying: What Is It and How to Stop It | UNICEF*, https://www.unicef.org/stories/how-to-stop-cyberbullying (last visited Oct. 8, 2025).
[18] *Ibid.*

ISSN: 2582-6433

on the Internet.[19] These readings give a legal background to tackle the different types of online violence but they also reveal how challenging it is to enforce the law in the offline space to the dynamic online space.

The Bharatiya Nyaya Sanhita (BNS) is an addition to the IT Act that concerns online abuse. In section 78, we find the definition of stalking which has been further expanded by the courts to have constant harassment via the Internet. Section 356 and Section 351 are the defamation and criminal intimidation of the electronic means, Section 79 protects women against verbal or non-verbal offenses that are aimed at attacking their modesty. The next section 196, 299 and 353 punishes crimes of injuring enmity, arousing hurt to religious emotions, or stimulating chaos among people including the cyber world. But the overlapping of jurisdiction and the procedural ambiguity tends to stand in the way of enforcement, victims are usually placed at risk of time and random results.

The legal intervention has played a key role in sensitizing the Indian response to the online violence. The classic case Shreya Singhal v. Union of India (2015), the court declared Section 66A of the IT Act has been unconstitutional as it violated Article 19(1)(a) of the Constitution and a precedent to balance freedom of speech and the right has been set against the harm. Several other cases have endorsed the idea of cyberstalking and cyberharassment as actionable offenses due to the fact that cyber abuse cannot be a symbolic offense and can result in real psychological and social damage.[20]

At the international level, treaties and conventions are meant to establish a sense of legality of complying with cyber crimes. The Budapest Convention on Cybercrime (2001) gives transborder cooperation in investigating cybercrimes like online harassment and abuse. The human rights council of the United Nations has rendered gender-based violence, which has been enhanced by technology, a human rights violation forcing states to incorporate end-to-end digital safety models. The elements of gender-based violence have been transferred to digital and online space in General Recommendation No. 35 of the Convention on the Elimination of All Forms of Discrimination Against Women, the idea of online abuse as a form

[19] *About the Convention - Cybercrime - Www.Coe.Int*, CYBERCRIME, https://www.coe.int/en/web/cybercrime/the-budapest-convention (last visited Oct. 8, 2025).
[20] Athena D. F. Sherman et al., *Discrimination, Sexual Violence, Depression, Post-Traumatic Stress Disorder, and Social Support among Black Women*, 34 J HEALTH CARE POOR UNDERSERVED 35 (2023).

ISSN: 2582-6433

of structural abuse of rights has been conceptualized.[21]

These models notwithstanding, a number of challenges still exist. The jurisdiction limitations come in where the offenders belong in other states and law enforcement is hard based on the domestic legislation. Gathering evidence of online crimes is difficult because of the anonymity, encryption, and the platform regulation. The fast-moving character of the technology has a tendency of exceeding legislative adjustments and must apply the law that has not been practiced before to similar circumstances. Digital intermediaries like social media networks and messaging applications also have questions of responsibility that are presented as special. Section 79 of the IT Act continues to provide conditional protection to the intermediaries, although the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021, which introduces due diligence and grievance redress, signifies the shift to joint responsibility, which means that the latter should also be included in the scope of the former.[22] Researchers also use a rights-based approach to improve law interventions, including an approach that is based on constitutional protection alongside the particular digital protection. This involves revising the available laws to be capable of responding directly to the increase in threat in deepfakes, AI-assisted harassment and non-consent sex pictures. Judicial alertness and anticipatory interpretation are also important and it should be ensured that the law acknowledges the presence of the harm of online violence as an actual and viable damage.

In conclusion, the Indian legal framework that is supplemented by international standards offers a background system to resolve the problem of online violence. Nonetheless, the implementation lapses, procedures-oriented peculiarities, and technological modernization are related to the fact that the laws and policy are never static. The legal approach should be supplemented by social policies, the responsibility of the platform, and educational courses to ensure a complete security of the citizens in the cyber environment.[23]

Roles of Social Media Sites and Digital Intermediaries

This expansion of social media and digital intermediaries has entirely transformed

[21] Muaadh Mukred et al., *The Roots of Digital Aggression: Exploring Cyber-Violence through a Systematic Literature Review*, 4 INTERNATIONAL JOURNAL OF INFORMATION MANAGEMENT DATA INSIGHTS 100281 (2024).
[22] Adrianne Saplagio, *Online Platforms Now Required to Safeguard Content*, COMMSROOM (Jan. 13, 2025), https://commsroom.co/preventing-harm-online-platforms-now-required-to-safeguard-content/.
[23] Lingxi Li, Jana Patricia M. Valdez & Yingqiao Du, *Digital Citizenship Education at the Early Childhood Level: How Is It Implemented? A Systematic Review*, 19 INTERNATIONAL JOURNAL OF CHILD CARE AND EDUCATION POLICY 13 (2025).

ISSN: 2582-6433

communication, distribution of information and the debate. Although the platforms offer social interaction spaces, learning platforms, and platforms to enact activism, it has equally become a platform of online violence through the form of harassment, hate speech, disinformation, and deliberate abuse. One should be in a position to know how these intermediaries play the role of dealing with the topic of online violence, socially and legally.

The online platform also contains intermediaries and the intermediaries are the social media websites, which includes, X (previously Twitter), Facebook, Instagram and YouTube. Section 79 of information technology act, 2000 gives the intermediaries conditional immunity against the third party contents liability as long as they exercise due diligence and follow the guidelines published by the government. The ideas of the grievance redressal, prompt access to unlawful content, and traceability provisions of big social media intermediaries are presented in Intermediary Guidelines and Digital Media Ethics Code Rules of 2021. Such regulations have been a step forward to collective responsibility between the state power and the individual platform on preventing online abuse.[24]

In the case of coded hate speech or sarcasm or veiled harassment (say) this may circumvent an automated screen and subject the victim to this kind of attack. And when on global platform, enforcement is not easily done in the sense that the hosted content on other countries may be out of the jurisdiction of the country.[25] The Supreme Court of India has also recognized that the privacy and dignity freedoms are equally violated as the digital media is allowed to be freely abused and the state has the duty to offer a secure digital arena.[26]

At the global scale, the regulatory frameworks tend to concentrate on the various approaches to accountability to the middlemen. European Union Digital Services Act (DSA) introduces more responsibility on platforms, such as in the shape of risk assessment, open content moderation, and penalties. Australia will be actively controlled as eSafety Commissioner is required to delete harmful information and directly assists the victims. The models demonstrate that platform responsibility is the socially and legally necessary

[24] Nicola Henry & Gemma Beard, *Image-Based Sexual Abuse Perpetration: A Scoping Review*, 25 TRAUMA VIOLENCE ABUSE 3981 (2024).
[25] Rebecca Dennehy et al., *The Psychosocial Impacts of Cybervictimisation and Barriers to Seeking Social Support: Young People's Perspectives*, 111 CHILDREN AND YOUTH SERVICES REVIEW 104872 (2020).
[26] Digital Violence Against Women: Is There a Real Need for Special Criminalization? | International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique, *supra* note 18.

ISSN: 2582-6433

phenomenon and that the cooperation between the regulators, civil society, and technology suppliers is one of the conditions.[27]

In simple terms, the social media and online facilitators are the regulators and facilitators of the online communications. It has a history of responsibility by relevant legal provisions like the IT Act Section 79 and the Intermediary Guidelines but regulation and balancing of the free speech and safety against harm and control remain a task. A harmonious freedom of legal regulation, of the technical responsibility and of the social awareness programs are necessary, in order to make the platforms not only a channel of communication, but also a zone of safety of all people.[28]

Preventive Response and mechanisms in the society

The fight against internet violence should be done beyond the realms of the legal system; however, it should be a multi-level social intervention consisting of governmental intervention, civil society intervention, technological protection and sensitization efforts. The legislation has been successful in holding individuals responsible but the social aspect is important in preventing, reducing and responding to cyber- bullying.

The role of government and regulatory bodies can also be of great importance of putting in place institutional mechanisms of countering online violence. Cybercrimes like stalking through posting intimate photographs without consent has a cybercrime cell dedicated by the state police forces in India. The National Commission of Women (NCW) and National Commission of Protection of Child Rights (NCPCR) have developed specific portals and redressal systems, using which the online abuse can be reported and tracked in real time. These organizations too carry out outreach campaigns to sensitize the citizens on online threats and justice in the law courts.

The civil society organizations are the complements of the state efforts as they create awareness, educate the vulnerable populations and lobby to reform the policy. The NGOs such as CyberPeace Foundation, Save the Children India, and Internet Democracy Project offer

[27] *The Judiciary's Tryst with Online Gender-Based Violence: An Empirical Analysis of Indian Cases and Prevalent Judicial Attitudes | IT for Change*, https://itforchange.net/judiciarys-tryst-online-gender-based-violence-an-empirical-analysis-of-indian-cases-and-prevalent (last visited Oct. 8, 2025).
[28] Digital Violence Against Women: Is There a Real Need for Special Criminalization? | International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique, *supra* note 18.

ISSN: 2582-6433

training programs on internet safety, cyberbullying prevention workshops, counseling, and legal support of the victims. These efforts target the digital literacy process such that citizens are able to work in the online space free of threats and be aware of their rights and responsibilities.

Education is one of the preventative measures. It is through the inclusion of the digital citizenship study in learning institutions, colleges, and other community programs that makes the capacity to detect, report, or oppose internet harassment possible. The awareness of suffering the effects of cyberbullying, image abuse, and hate speech on the Internet makes the abusive behavior less acceptable and compassionate on the Internet. First, there are more platforms and non-governmental organizations declaring reporting routes, filters by parents, and educative programs to make internet a safer place.

Lessons of valuable comparative international models exist. A case in point is the eSafety Commissioner of Australia which is a holistic model with education, enforcement, and victim support services to the victims of online harassment. Digital Services Act of the European Union requires significant reporting and takedown procedures of intermediaries, and a scheme of shared accountability amid regulators, platforms and users. These external models show that the prevention measures must be effective in combining legal, social, and technological means in their prevention efforts.

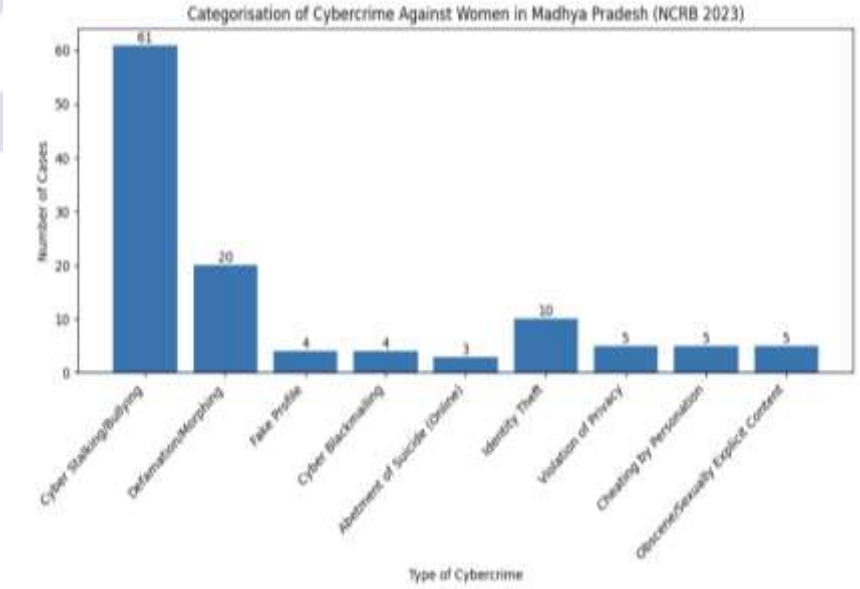
In most cases, the society reacts to violence on the internet in a multi-stakeholder strategy that involves governments, civil society, schools, platforms, and communities. The statutory law has been accompanied by preventative measures, educative measures and support to victims. Social education, legal recourse and technical actions are the only factors that will provide a conducive environment that will reduce the harm caused online, which will also increase digital literacy and responsibility between the platform and the user.

Cybercrime agaisnt Women in Madhya Pradesh

The most recent NCRB Cybercrime Report 2023 indicates that there were 685 cases of cybercrime in Madhya Pradesh with a projected population of 869.2 lakh which represents a very low cybercrime rate of 0.8 per lakh population; the state was however very efficient in terms of its institutions as it had a high chargesheeting rate of 93.7 percent.

ISSN: 2582-6433

According to the report cybercrime against women in the state is largely dominated by harassment- and privacy-related crimes but not massive monetary frauds. Section 354D IPC (outlined the highest profile of cybercrime committed against women) 61 cases of cyber stalking and online bullying of women and children were recorded in the state. This was preceded by 20 cases of online defamation and morphing where the image or personal details of women were abused to create a bad reputation on the internet. Also, fake profile creation and cyber blackmailing or threatening cases were 4 each, which is the reason why the use of social media as an intimidation instrument and coercion tool against women has become widespread. Criminal activities that were directly related to women under the Information Technology Act were 10 cases of identity theft (Section 66C), 5 cases of violation of privacy (Section 66E), 5 cases of cheating by personation using computer resources (Section 66D) and 5 cases concerning the publication or transmission of obscene or sexually explicit content (Section 67), one of which involved child sexual abuse material.



In general, the statistics indicate that cybercrime against women in Madhya Pradesh is mostly predetermined by the personal vengeance and the conflicts between individuals. The motive-wise analysis also shows that personal revenge was the major motive behind cybercrimes in the state with 102 cases mostly being motivated by this factor, fraud and sexual exploitation were relatively low. On the whole, the statistics show that whereas the number of cybercrime reported in Madhya Pradesh is notably lower, cybercrimes targeting women are more likely to be harassment-, privacy-, and reputation-related, which means that further awareness, reporting systems, and gendered cyber policing should be maintained despite the high result of investigations and prosecutions in the state.

ISSN: 2582-6433

Judicial Reactions and Path-Breaking Case Laws on Cyber Violence

The cyber violence has taken a new twist and law has been enforced by judicial system in the cyberspace. The world courts and the Indian courts specifically have been finding an increasing significance on the fact that the abuse mediated by technology can be said to be real harm and not abstract harm and a real violation to the rights of the individual. Not only does the statutory prerequisites get the judicial decision, but also the sizes of the constitutional guarantees such as the privilege of privacy, the freedom of speech, and the freedom of equality.

In India, cybercrime against women has developed to become a sophisticated legal issue involving online harassment, violation of privacy, identity abuse, and sexual exploitation. Often, Indian courts have taken a progressive step to consider these offences through the prism of the provisions of the IPC, IT Act, 2000, to respond to new types of digital abuse and offer legal protection as the result of technological abuse.

The most obvious case is that in India, that is, Shreya Singhal v. Union of India (2015) 5 SCC 1 in a case in which the Supreme Court has declared the Section 66A of the Information Technology Act, 2000, as unconstitutional. The Court stated that Section 66A was vague and unreasonable because it infringed Article 19(1) (a) (freedom of speech). Surprisingly, the case in point has brought in the contradictory aspect of policing obscene materials online and the promotion of free speech because it has established precedence in balancing the rights in the online sphere.

The IT Act brought to the limelight of The Supreme Court in Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473 the digital evidence. The Court explicated that the electronic records have to be genuine and believable that will lead to the challenges of evidence in the setting of online violence, specifically, cyber defamation and instances of online harassment. The Court repeated cyber abuse is a grave abuse of the right to privacy (Article 21) but also the right to dignity, and that needs to be taken to task through legal action nowadays, and law enforced by the police in such proceedings.

In Srinivas Rao v. D.A. Deepa (2013) the Madras High Court expressly construed cyber stalking and online harassment as a type of sexual harassment and made such behaviour subject to the provisions of the Indian Penal Code as provided in Section 354A. This judicial decision was also enforced in the case Manish Kathuria v. Ritu kohli (2014) a case of reported cyber

ISSN: 2582-6433

stalking and cyber sexual harassment was the first of its kind in India with the elements of impersonation by means of using falsified online accounts that misused personal information being found to violate the modesty of a woman as defined in section 509 of Indian criminal law and hence was the beginning of the acknowledgement of cyber harassment as a form of serious gender based crime.

The issue of harassment and impersonation through social media networks was particularly covered in the case of Prakhar Sharma v. The case of State of Madhya Pradesh (2018), when the accused made a fictitious profile with the help of a photograph of the victim and posted obscene information with a bad motive. The Madhya Pradesh high court denied bail because the accused was charged with guilt as categorized in Section 66C, 67 and 67A of Information technology act, 2000 thereby confirming that identity theft and obscene digital publication are really a serious cyber crime directed at women.

Online defamation and morphing have also been viewed as serious offenses that courts take into consideration when it comes to the issue of dignity and reputation. In S. Khushboo v. Kanniammal, the Supreme Court recognized the chilling effect of defamatory online speech on the autonomy and dignity of women. Likewise, the State of Tamil Nadu v. Suhas Katti (2004) was the first case to be convict in India where the defendant was found guilty on cyber defamation and cyber pornography under the provisions of Section 67 of the IT Act and Sections 509 and 469 IPC of publishing defamatory and obscene content against a woman. The rapid conviction on the case indicated that the court was willing to deal with cyber crimes that tarnish women.

The courts have been strict on the cases where there has been coercion and sexual misappropriation over the internet. In State v. Madachirayil Gopinathan Suni (2018), accused tried to get sexual favors and threatened to spread morphed pictures. The court affirmed the conviction of Sections 506, 507, and 509 IPC as well as Section 67 of the IT Act and it was clearly stated that digital threats and non-consent circulation of images were types of criminal intimidation and insult to modesty.

Judicial handling of fake profile making and identity theft have been considered as two specific cyber crimes. At the same time, quashing Section 66A of the IT Act in Shreya Singhal v. The Supreme Court (2015) made it clear that the identity theft and impersonation offences

ISSN: 2582-6433

of Sections 66C and 66D cannot be dismissed due to their validity and sanctionability. This clarification has been applied in subsequent cases by repeately relying on it, such as Prakhar Sharma v. The State of Madhya Pradesh (2018), strengthening the accountability on digital impersonation of women.

Cyberspace has provided women with great protection in court due to the judicial awareness of privacy breaches. In Justice K.S. Puttaswamy v. Union of India (2017), the constitutional right to privacy came into being applied in cybercrime cases. In X v. The court, State of Maharashtra (2023) found that the act of sharing of personal pictures without the consent of the parties is a violation of Article 21 of the Constitution, as well as of Section 66E of the IT Act. In a previous case, State of Maharashtra v. Yogesh Prabhu (2009), a person accused and convicted on Sections 66E IT Act and 509 IPC of stalking and publishing obscene digital content affirmed that intruding into the personal life of a woman online is a punishable offence.

Courts have taken a victim-focused approach in the cases of obscene and sexually explicit materials. In State of West Bengal v. Animesh Boxi (2018), the circulation of intimate images without consent was defined as virtual rape, which is quite a precedent established by to treat revenge pornography as a serious sexual crime. In ABC v. State (Madras High Court, 2022) this principle was restated enhancing judicial security of women body online. On the same note, Jayanta Kumar Das v. State of Odisha (2017), the accused was found guilty of offenses in Section 67A of the IT Act in publishing obscene content and mentally harassing people through online platform.

Sextortion and cyber blackmailing have also been denounced by the courts. The Supreme Court in Re: Prajwala Letter Case (2021-23) highlighted the need to have coordinated cyber-policing processes to deal with online sexual exploitation. In Saddam Hussain v. State of Madhya Pradesh (2016) the accused was found guilty of offences in accordance with Section 67 of the IT Act, and 506, 507 and 509 IPC in terms of recording and distributing obscene material to threaten the victim and coerce into sex, which reiterates that any attempt of digital manipulation and control is severely punishable with criminal penalties.

Cyberspace abuse has also been shown with more finesse at the international level too. In the Case of Delfi AS v. Estonia (2015) the site was found guilty of defamatory statements

ISSN: 2582-6433

by its users according to European Court of Human Rights, the ECHR because it did not take down the toxic content after discovering its presence. The case presents the responsibility of middle people in minding abusive content. In Lilly Singh v. The case of social media, Twitter Inc. (2021, Canada) was compelled to deal with the issues of harassment and threats that were occurring online, which proved that online abuse imposes a physical impact and social media may be held liable to carry the damage.

The courts always interpret online violence as real harm. Constitutional rights especially privacy, dignity and freedom of expression are in the fore-front in the trade-off between regulation and enforcement. The online mediums are the ones that are increasingly being blamed as the facilitators or failure to prevent the abuse. The quality of digital evidence must be of superior quality of authenticity and reliability. Judicial discourse suggests that law is not adequate but the courts can have major role to play in interactive interpretation of laws with regard to the technological change. On the whole, it can be concluded that judicial trends indicate that Indian courts gradually broaden the scope of the interpretation of available laws in response to cybercrime against women. The case law indicates a drastic change of perspective on such offences as the technical violations to the status of serious crimes that impact dignity, privacy and mental health. This legal philosophy emphasizes the pressing necessity of effective legal regulations and online consciousness. The indication of judicial activism in online violence cases is the presence of a desire to shield vulnerable groups especially women and marginalized groups against technology enabled harm.

Recommendations and Conclusions

The social, psychological, and legal consequences of such phenomenon as cyber violence are terrible, even when it occurs with the assistance of online platforms. It goes beyond the walls of the virtual space to the fields of dignity, privacy, and well-being of an individual in a physical world. Online violence as it has been established in this paper is not a vice per se, but it is an image and a reflection of other misfortunes of society e.g. gender discrimination, caste and community prejudices, and marginalization of the weak. The relationship between the society, technology and the law is thus extremely high in solving this complex problem.

On the legal side, the legislative base of India that encompasses the Information Technology Act, 2000, Indian Penal Code, Bharatiya Nyaya Sanhita (BNS) and so on, gives a platform to start with in regulating violence in the internet. Courts in cases like Shreya Singhal

ISSN: 2582-6433

case the constitution has drawn distinctions between the freedom of expression and the right to remain safe. However, there are still loopholes in the enforcement, gaps in technologies, and a lack of jurisdiction. The international instruments like the Budapest Convention on Cybercrime, the resolutions of the UN Human Rights Council and the CEDAW General Recommendation No.35 provide a relative understanding where internet violence is a human right issue that must be addressed with an optimistic and organized approach. Further, Madhya Pradesh has quite a low level of cybercrime rates in general, but the NCRB-data indicate that a large proportion of cyber crime against women can be associated with harassment, stalking and privacy invasion. Such crimes are under-reported or improperly handled in most cases as they lack specialized support.

There is need of out of courtroom intervention in online violence. The awareness, digital literacy and community based preventive measures are extremely pressing in empowering the user and facilitating resilience. The mentioned educational programs that would focus on the responsible digital citizenship, the efficient reporting mechanisms, and the guidance mechanism can mitigate the impacts of the abuse and prevent the normalization of the pernicious conduct. These kinds of platforms and other online mediators must find that balance between freedom of speech and active moderation, visibility and responsibility, and ensure that the technological design does not inadvertently support abuse.

According to the provided analysis, it is possible to give several recommendations that are important:

- **Improving Law and Order:** Enact certain laws to deal with the menace of deepfakes, AI-assisted harassment, and stalking on the basis of cyber-facilitation in the future. Increase transparency of the procedures and offer an effective cross-border implementation.
- **Increase Platform Accountability:** Enforce strong grievance redressal mechanisms, open content moderation, and algorithmic audits to eliminate systemic amplification of abuse.
- **Enhance Digital literacy and Awareness:** Integrate the notion of digital citizenship, cyber ethics and online safety by educating across the board to create awareness to the vulnerable groups. Further, the state of Madhya Pradesh ought to initiate easy cyber safety education to women and the young population, aiming at safe usage of the social media, protection of privacy, detection of a counterfeit profile and easy reporting of cybercrime.

ISSN: 2582-6433

- **Support Victims:** The psychological support, legal services, and safe reports services should be provided to the victims to make sure that the social and emotional consequences of online violence are reduced to their minimum.
- **Create Multi- Stakeholder Partnership:** Instigate partnership among the governments, civil society, academia and technology providers to develop a collective responsibility system.
- **Establish cybercrime cells:** Madhya Pradesh ought to also come up with special women oriented cybercrime cells in all the districts so that the victim does not take long to report, issues of cyber offences as well as cyber harassment against women can be dealt with as it can be addressed properly.

Finally, online violence cannot be dealt with by legal means. It should be a holistic, rights-oriented approach of incorporating law, technology, learning and social conscience. The point of these spheres can respond to it only in case the society makes sure that virtual spaces are safe, complete, and contribute to the enforcement of primary rights. Online violence that transcends the screen is therefore not only a legal and required minimum but a social mandate and is meant to safeguard human dignity and fair utilization of the digital era.