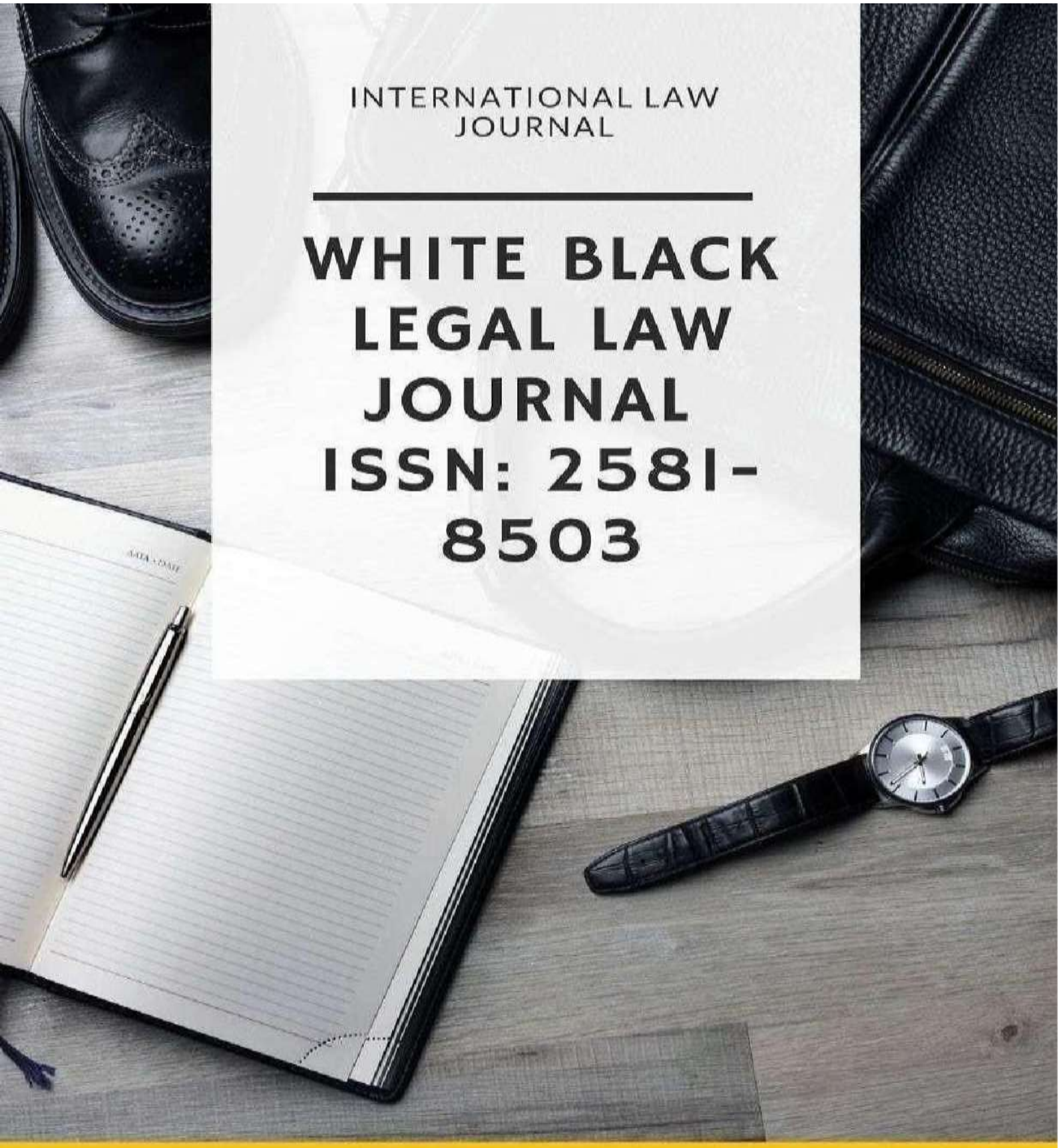

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

CYBERBULLYING AGAINST WOMEN: DOCTRINAL GAPS, COMPARATIVE LESSONS, AND REFORM PATHWAYS

AUTHORED BY - ALEXANDER. C
Research Scholar, School of Law
Vel Tech Rangarajan Dr. Sagunthala
R&D Institute of Science and Technology,
Avadi, Tamil Nadu 600062

CO-AUTHOR - DR. B. VENUGOPAL
Professor & Dean, School of Law,
Vel Tech Rangarajan Dr. Sagunthala
R&D Institute of Science and Technology,
Avadi, Tamil Nadu 600062

Introduction

Digital spaces have taken over the social, professional, and political lives of women, but they have also escalated the experiences of gendered abuse, harassment, and humiliation online. [1]Cyberbullying of women includes a continuum of actions such as threats of rape or death, non-consensual release of intimate images, doxing, morphing, impersonating, and organizing trolling campaigns, all of which primarily affect women and gender nonconforming individuals who give speeches. The article suggests that these harms cannot be considered incidental side effects of online speech and that they are a structural manifestation of gender-based violence, which current legal frameworks either overlook or fail to effectively control.

The discussion is based on a doctrinal, comparative and empirically informed perspective. It also establishes the basis of cyberbullying of women amid the international standards of violence against women and freedom of expression, and follows the response of Indian legislation on the subject through the Information Technology Act 2000 (IT Act), the Indian Penal Code 1860 (IPC), and others. It subsequently uses comparative strategies of the United Kingdom, the United States[2] and the European Union to determine criminalization, intermediary and platform governance models. The article incorporates empirical study to demonstrate that enforcement is still lax, under-reporting is ample, and cross-cutting differences are intensive. It ends with normative and institutional reform suggestions that attempt to balance strong protection against cyber-violence with constitutional obligations to

[1] Nadim M, Fladmoe A (2021) Silencing women? Gender and online harassment. Soc Sci Comput Rev 39(2):245–258.
[2] Convention on the Elimination of All Forms of Discrimination against Women, Dec. 18, 1979, 1249 U.N.T.S. 13.

free expression and due process.[3]

Normative and Conceptual Foundations

Cyberbullying as gender-based violence

This is a developing trend: the international human rights law has come to appreciate the use of technology-mediated abuse as a type of gender-based violence that involves the state due diligence, prevention, investigation, and redress duties. The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the General Recommendations No. 19 and 35, also conceptualize violence against women as a result of historically unequal power relations and demands that states tackle both online and offline violence against women. On the same note, the UN Declaration on the Elimination of Violence against Women and reports of the UN Special Rapporteur on violence against women have highlighted that online harassment, non-consent image sharing and online stalking are in the spectrum of gendered harms.[4]

According to the feminist legal theory, cyberbullying of women is not a series of individual interpersonal injustices but a system of social control that regulates the visibility of women, their sexuality, and their dissent. Women journalists and politicians, Dalit and Adivasi women, queers and human rights defenders are common targets of online abuse, thus shutting off the inclusion in the democratic process and strengthening structural subordination. These trends encourage the thinking that cyberbullying is more of discrimination than violence, which explains the increased intervention of the state in comparison with the normal interpersonal insults or disagreements.[5]

Free speech, privacy, and dignity

Response to cyberbullying by the regulator should be in such a manner that the three components of free speech, privacy and dignity are addressed. In India, the centrality of the internet to the right to freedom of speech and expression under Article 19(1)(a) of the Constitution has been recognized by the Supreme Court, and over broad restrictions like the now outdated section 66A of the IT Act have been struck down in Shreya Singhal v. Union of India. Meanwhile, the Court has discussed a strong constitutional right to privacy and

[3] United Nations. (1993). Declaration on the elimination of violence against women (A/RES/48/104).
[4] United Nations Committee on the Elimination of Discrimination against Women. (2017). General Recommendation No. 35 on gender-based violence (Updating No. 19).
[5] World Health Organization. (2013). Global and regional estimates of violence against women.

informational self-determination in K.S. Puttaswamy v. Union of India, sexual autonomy and decisional privacy as fundamental interests.[6]

The instances of cyberbullying are associated with the direct conflict between these values. The misogynistic trolling or revenge pornography is perpetrated with the aid of free speech, whereas the victims of cyberbullying protect their privacy, dignity, and equality. A good regulatory system should thus draw a line between [7]the coverage of the controversial or offensive opinion, which is the focus of the democratic discourse, and the intended, systematic and gendered abuse aimed at silencing or terrifying. It should also realize the influence of platforms as privatized regulators of the online environments and compel them to combat cyber-violence by transparent, rights-respecting content moderation and design decisions.

Doctrinal Landscape in India

Substantive criminal provisions

Cyberbullying of women is dealt with by the Indian criminal law as a patchwork of offences under the IPC and the IT Act as opposed to a technology-specific law. IT Act includes unauthorized access, data stealing, and publication/ transmission of sexually explicit content, being 66E (violation of privacy), 67 (obscenity), and 67A-67B (sexually explicit and child sexual abuse material). This can, and has been, applied to non-consensual sharing of intimate images, morphing and voyeuristic secretive videos.[8]

The IPC complements them with gender-specific offences as stipulated in the criminal law (amendment) act 2013, including section 354A (sexual harassment), section 354C (voyeurism), and section 354D (stalking), specifically stating that electronic communication is included in the scope of these acts. Most of the forms of cyber-harassment are also covered in sections 499-500 (criminal defamation), 503-507 (criminal intimidation and anonymous communication), and 509 (insulting the modesty of a woman). Ideally, this dogmatic edifice allows the [9]prosecution of a wide scope of online abuses, but there is space and vagueness.

Intermediary liability and safe harbors

An important aspect of cyberbullying regulation is the liability of the intermediaries like the social networking sites, messaging service and web-hosting service providers. The IT Act

[6] Information Technology Act, 2000 (India).
[7] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
[8] Communications Decency Act, 47 U.S.C. Sec 230 (United States).
[9] Violence Against Women Act of 1994, Pub. L. No. 103-322.

provides conditional safe harbor (under section 79) to intermediaries against liability of third-party content on the basis that they exercise due diligence, they publish rules and policies and take expeditious action on lawful requests or when they have actual knowledge of illegal content. In 2021, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 broadened these requirements greatly to provide grievance redressal tools, timely takedown of content in cases of actual knowledge, and in some respects traceability of message senders.[10]

Although these regulations are potentially beneficial to accessing prompt relief by victims, they present due process and privacy objections. Combined with the risk of loss of safe harbor, open-ended takedown obligations can encourage excessive removal of content, such as feminist or queer speech and expression which is falsely reported as obese or anti-national. Encrypted messaging service traceability needs also pose the threat of breaching confidentiality and may be used against vulnerable populations. The current regime thus will not have a victim-focused norm of accountability of platforms concerning gender-based cyber-violence.[11]

Constitutional constraints and judicial responses

There are significant limitations put on legislative and executive action against cyberbullying in the jurisprudence of the Supreme Court. The Court in Shreya Singhal stated that limitations on online speech should not exceed Article 19(2), but they should be narrow and should not be open to interpretation and silence the [12]rightful expression. This argument highlights the impossibility of using such broad and subjective terms as annoyance or inconvenience in criminalizing online speech as was previously the case. The new cyberbullying specific offence should be henceforth defined cautiously with emphasis on targeted, persistent, and gendered behavior as opposed to just general offensiveness.

Meanwhile, the Court has recognized the validity of privacy and dignity safeguarding in online environments by including the right to be forgotten in some situations and issuing orders to have non-consensual intimate content de-indexed by search engines. The possibilities and boundaries of the judicial remedies have been matched by an increase in petitions before the high courts by women demanding that morphed images, fake profiles, and sexually explicit videos be deleted. They demonstrate not only a judicial desire to develop ad hoc remedies but also the lack of an overarching statutory framework that explicitly acknowledges technology-

[10] Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), ETS No. 185.
[11] Violence Against Women Act of 1994, Pub. L. No. 103-322
[12] European Union. (2016). General Data Protection Regulation (GDPR) (EU) 2016/679

enabled gender-based violence.[13]

Comparative Legal Responses

United Kingdom

The United Kingdom has dealt with offenses of abuse online by a mixture of older communications offences and new reforms. The Malicious Communications Act 1988 and the Communications Act 2003 in section 1 and section 127 respectively, [14]criminalize sending messages that are grossly offensive, indecent, obscene, or threatening whether by using electronic communication systems or not. Guidelines of prosecutors and caselaw have attempted to restrict such provisions to serious and recurrent abuse, although the issue of excessive breadth and inconsistent application remain.[15]

More recently, the UK has introduced the Online Safety Act 2023, which introduces a statutory duty of care on large platforms to reduce the risk posed by unlawful and harmful yet lawful content, such as abuse against women and girls. This Act imposes risk assessment, content moderation systems, and user-empowerment tools, which are under control of Ofcom as an independent regulator. Though the mechanisms of implementation are disputed, this infrastructure-centered paradigm lets the focus off individual criminal responsibility and focuses on systemic responsibility of platforms, and introduces complicated free-speech and novelty dilemmas.[16]

United States

Cyberbullying is a part of criminal law that is disjointed in the United States both at the federal and state levels. Cyberstalking, threats, and other type of harassment have been prosecuted using federal laws like the Interstate Stalking Punishment and Prevention Act and the Violence Against Women Act (VAWA) especially when interstate communication or a protected classes are used. Many states have passed bills on cyberbullying or cyber-harassment, most frequently regarding youth and school situations, but which have been objected to as being too broad and vague.

Simultaneously, the Communications Decency Act, Section 230, gives content indirect

[13] Citron, D. K. (2014). Hate crimes in cyberspace. Harvard University Press.
[14] MacKinnon, C. A. (1989). Toward a feminist theory of the state. Harvard University Press.
[15] Barendt, E. (2005). Freedom of speech (2nd ed.). Oxford University Press.
[16] Wright, M. F. (2016). Cyberbullying victimization & adjustment difficulties. Journal of the Association for Information Science and Technology, 67(5), 1015–1027.

participants in the internet a wide-ranging immunity against civil and criminal actions by users and even in instances of egregious gendered abuse. Although this safe harbor has been justified as a crucial part to freedom of expression and innovation, feminist scholars present the view that it outsources the cost of online misogyny onto women and marginalized users. Reform proposals to amend Section 230 are getting more and more focused on gradually creating exceptions to deal with the most extreme types of cyber-violence, specifically non-consensual pornography, but still maintain protection of good-faith moderation.[17]

European Union

The European Union has been using technology-mediated violence by regulating digital services and gender-equality tools. General Data Protection Regulation (GDPR) gives individuals rights to erasure and limitations to processing which have been used to suspend non-consensual intimate material and other malicious content. The Digital Services Act (DSA) 2022 refers to very large online platforms that have a due-diligence obligation including risk assessment, systemic risks mitigation, and disclosure of content moderation and recommender systems.

Simultaneously, the Istanbul Convention of the Council of Europe directly acknowledges psychological violence, stalking, sexual harassment, and sexual violence, even mediated by technology, and obligates state actors to criminalize the aforementioned acts and offer effective solutions. Draft EU guidelines against violence against women and domestic violence attempt to bring countries in line by criminalizing cyberstalking, cyber-harassment, sharing images without consent and incitement to violence or hatred grounded in sex or gender. These changes portend a shift to what is explicitly termed and actuated on the regional human rights and criminal law levels in relation to gender-based violence on the Internet.

Empirical Realities and Enforcement Gaps

Prevalence and patterns of harm

The empirical research in the area of jurisdictions has revealed that the rates of technology-mediated abuse of women are high, and the burdens affect young women, women with intersectional identities, and those in the public spotlight like journalists and politicians unequally. Indian and international surveys show that large percentages of women who use the

[17] Wright, M. F. (2016). Cyberbullying victimization & adjustment difficulties. Journal of the Association for Information Science and Technology, 67(5), 1015–1027.

internet have received sexualized threats, unwanted explicit pictures, impersonation and organized trolling efforts, frequently through multiple sites. The mental and social after effects include anxiety, depression, retreating to social conversation, self-censorship and in the worst extreme abandoning the country or abending a profession.[18]

Offline risks compound these harms. Physical stalking, domestic abuse and honor based violence can be expedited through doxing, sharing of locations, and distributing intimate images. Online abuse usually combines misogyny with casteism, communalism, homophobia, and transphobia as it is experienced by Dalit, Adivasi, Muslim, queer, and trans women, demonstrating how cyberbullying recreates intersectional hierarchies. Nevertheless, cyber-violence against women is often under-reported in official statistics of crime as it is mistaken, mis-classified, [19]and lacks specific categories.

Barriers to reporting and redress

Female avenues to the law are blocked in various levels. Most victims do not report because they are afraid of the stigma, victimization, victimizing and because they do not trust police knowledge of digital evidence. Anecdotally, and empirically, complaints made usually result in police proving to downgrade online abuse as virtual or private feuds, discouraging the filing of First Information Reports (FIRs) or pressurizing inappropriately to compromise or get married.[20]

The investigation of cyber-offences is procedurally demanding specialized skills and technological tools, as well as, cross-jurisdictional cooperation which local police stations often lack. Sluggishness in obtaining platform data, absence of standard operating procedures on evidence preservation and jurisdictional differences between states and even countries all lead to low conviction rates. Where courts issue takedown or restraint orders, in part because of the viral and replicative nature of digital content, the complete elimination of content is hardly a possibility, an issue that creates the impression of constant powerlessness in survivors.[21]

Platform governance shortcomings

The responses of platform to cyberbullying of women are disproportional and obstructed. The

[18] Patchin, J. W., & Hinduja, S. (2015). Bullying beyond the schoolyard (2nd ed.). Sage.
[19] Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying beyond the schoolyard. Psychological Bulletin, 140(4), 1073-1137.
[20] Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying beyond the schoolyard. Psychological Bulletin, 140(4), 1073-1137.
[21] United Nations. (2015). Transforming our world: 2030 Agenda for Sustainable Development

content moderation systems tend to be insensitive to context-specific abuse, local languages, or intersectional slurs, which results in both a lack of enforcement in the face of severe abuse and excessive enforcement of feminist and queer activism. Automated detection tools are often trained on English language and Western data, foaming prejudices and blind spots of Global South users.

Transparency reports are usually summarized with no gender-disaggregated data on harassment and hate-speech, which conceals the actual weight of the burden on women and marginalized groups. Appeals systems are inefficient and do not truly involve any meaningful human consideration, especially to the Global South users. This is because the platforms do not have legally required, gender-sensitive risk management and independent audits that would compel them to consider gender-based cyber-violence as an act of corporate privilege instead of a rights-based requirement.[22]

Towards Gender-Responsive Reform

Clarifying offences and recognizing technology-facilitated violence

Doctrinally, the Indian law would do well to have a statutory acknowledgment of technology-aided gender-based violence as an independent category that will fill the gap between "cyber" and "offline" crimes. Instead of creating a general, speech-based cyberbullying crime, the legislature might modify the already existing law on stalking, sexual harassment, voyeurism, criminal intimidation, and defamation to include specific explanations and examples on crimes related to online behaviors, doxing, deepfakes, or threats with the help of organized campaigns.[23]

A definition of gender-based violence involving the use of technology, which is consistent with CEDAW and the Istanbul Convention, might be included in the IT Act or a special law to inform the interpretation, data gathering, and policy formulation. This definition needs to focus on the repetitive and gendered behavior that is likely to instill fear, humiliation, or significant interference in the enjoyment of a public life, as opposed to interpersonal conflict or isolated punishments of offensive material. This would lessen over-criminalization, but would at the same time embody the structuralism of cyber-violence against women.[24]

[22] United Nations Entity for Gender Equality and the Empowerment of Women (UN Women). (2021). Facts and figures: Ending violence against women

[23] Office of the United Nations High Commissioner for Human Rights. (2018). Guidelines for eliminating discrimination against women

[24] Amnesty International. (2018). Toxic Twitter: A toxic place for women.

Strengthening procedural and institutional capacities

There should be strong procedural protection and institutional strength to supplement substantive offences. The training of specialized cyber-crime units and women help desks to handle technology-facilitated abuse, trauma-informed interviewing, and digital forensic methods should be systematized. SOPs are required to ensure timely registration of FIRs, victim-based risk assessment, and liaise with platform grievance officers to ensure timely takedown and evidence preservation.

The legal aid services and one-stop crisis centers might be enlarged to provide targeted services to victims of cyber-violence, such as help with documentation, platform reporting, and assistance in overcoming the problem of cross-border jurisdiction. The data protection and privacy authorities are expected to come up with advice on how intimate pictures and sensitive personal information should be handled in that remedial measures taken should not further endanger the privacy of victims or their autonomy. Disaggregated statistics on cyber-violence against women should be reported in the country periodically to check the implementation and determine the differences in the region.

Re-designing intermediary obligations

Regimes of intermediate liability must be reviewed to introduce explicit, proportionate, and gender-sensitive responsibilities on platforms without eliminating end-to-end encryption or the rights of users to anonymity in relevant situations. Based on the EU Digital Services Act and UK Online Safety Act, the Indian law may need large platforms to complete a risk assessment based on gender every quarter and release comprehensive transparency reports on harassment and hate-speech legal action, and accessible, language-neutral reporting and reporting systems.[25]

Grievance redressal duties must put more emphasis on user safety without responding to platforms with quasi-judicial censorship. This may be done by using independent co-regulatory institutions or ombuds institutions that scrutinize systemic practices, overseeing complicated complaints, and making authoritative standards, instead of enacting general takedown requirements supported by criminal penalties. Any traceability or identification criteria should be only necessary, proportionate, and open to judicial scrutiny to avert abuse against activists, whistle-blowers, and victims of abuse who seek to remain anonymous.

[25] UNICEF. (2017). A familiar face: Violence in the lives of children

Beyond criminal law: education, design, and culture

Lastly, a long-term solution to cyberbullying of women cannot just be based on criminalization, but needs to be learning-based, platform engineering, and culture shifting. Schools and universities should teach digital citizenship that covers consent, gender equality and bystander intervention over the internet, with accompanying campaigns to raise public awareness, which de-stigmatizes reporting and counters the victim-blaming discourse.

Social media can be encouraged or mandated to implement safety-by-design features and protocols that include default privacy preferences, resistance to mass-messaging, confirmation before posting potentially harmful messages, and strong blocking and muting capabilities. Peer-support networks and documentation projects that provide resilience on a community basis have been developed by feminist civil society, journalist's unions and women groups and that ought not to be blocked by the law and policy. Identifying cyberbullying of women as a group, institutional problem and not a sequence of personal conflicts is a pre-condition to develop effective reforms that are rights-based.[26]

References (APA Style)

- Convention on the Elimination of All Forms of Discrimination against Women, Dec. 18, 1979, 1249U.N.T.S.13.https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women
- United Nations. (1993). Declaration on the elimination of violence against women (A/RES/48/104). https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/48/104
- United Nations Committee on the Elimination of Discrimination against Women. (1992). General Recommendation No. 19: Violence against women. https://www.refworld.org/docid/52d920c54.html
- United Nations Committee on the Elimination of Discrimination against Women. (2017). General Recommendation No. 35 on gender-based violence (Updating No. 19). https://www.ohchr.org/en/documents/general-recommendations
- World Health Organization. (2013). Global and regional estimates of violence against women. https://www.who.int/publications/i/item/9789241564625

[26] Smith, P. K., Mahdavi, J., Carvalho, M., & Tippett, N. (2008). Cyberbullying: Its nature and impact. Journal of Child Psychology and Psychiatry, 49(4), 376-385.

- Information Technology Act, l2000 (India). https://www.meity.gov.in/content/information-technology-act
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India). https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_Rules.pdf
- Communications Act 2003 (UK). https://www.legislation.gov.uk/ukpga/2003/21/contents
- Online Safety Act 2023 (UK). https://www.legislation.gov.uk/ukpga/2023/27/contents/enacted
- Communications Decency Act, 47 U.S.C. § 230 (United States). https://www.law.cornell.edu/uscode/text/47/230
- Violence Against Women Act of 1994, Pub. L. No. 103-322. https://www.congress.gov/bill/103rd-congress/senate-bill/254
- Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), ETS No. 185. https://www.coe.int/en/web/cybercrime/the-budapest-convention
- Council of Europe. (2011). Istanbul Convention. https://www.coe.int/en/web/istanbul-convention
- European Union. (2016). General Data Protection Regulation (GDPR) (EU) 2016/679. https://eur-lex.europa.eu/eli/reg/2016/679/oj
- European Union. (2022). Digital Services Act. https://eur-lex.europa.eu/eli/reg/2022/2065/oj
- Citron, D. K. (2014). Hate crimes in cyberspace. Harvard University Press. https://www.hup.harvard.edu/catalog.php?isbn=9780674057222
- MacKinnon, C. A. (1989). Toward a feminist theory of the state. Harvard University Press. https://www.hup.harvard.edu/catalog.php?isbn=9780674075727
- Zuboff, S. (2019). The age of surveillance capitalism. Profile Books. https://profilebooks.com/work/the-age-of-surveillance-capitalism/
- Barendt, E. (2005). Freedom of speech (2nd ed.). Oxford University Press. https://global.oup.com/academic/product/freedom-of-speech-9780199261948
- Wright, M. F. (2016). Cyberbullying victimization & adjustment difficulties. Journal of the Association for Information Science and Technology, 67(5), 1015–1027. https://doi.org/10.1002/asi.23436

- Ybarra, M. L., & Mitchell, K. J. (2008). How risky are social networking sites? Pediatrics, 121(2), e350-e357. https://doi.org/10.1542/peds.2007-1084
- Patchin, J. W., & Hinduja, S. (2015). Bullying beyond the schoolyard (2nd ed.). Sage. https://us.sagepub.com/en-us/nam/bullying-beyond-the-schoolyard/book243842
- Hinduja, S., & Patchin, J. W. (2010). Cyberbullying research summary. Cyberbullying Research Center. https://cyberbullying.org/2010_cyberbullying_research_summary
- Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying beyond the schoolyard. Psychological Bulletin, 140(4), 1073-1137. https://doi.org/10.1037/a0035618
- United Nations. (2015). Transforming our world: 2030 Agenda for Sustainable Development. https://sdgs.un.org/2030agenda
- United Nations Entity for Gender Equality and the Empowerment of Women (UN Women). (2021). Facts and figures: Ending violence against women. https://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures
- United Nations Children's Fund. (2020). State of the world's children 2020. https://www.unicef.org/reports/state-of-worlds-children-2020
- Office of the United Nations High Commissioner for Human Rights. (2018). Guidelines for eliminating discrimination against women. https://www.ohchr.org/en
- Amnesty International. (2018). Toxic Twitter: A toxic place for women. https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-toxic-twitter
- Pew Research Center. (2021). Americans and online harassment. https://www.pewresearch.org/internet/2021/01/13/americans-and-online-harassment/
- European Institute for Gender Equality. (2022). Cyber violence against women and girls. https://eige.europa.eu/publications/cyber-violence-against-women-and-girls
- UNICEF. (2017). A familiar face: Violence in the lives of children. https://www.unicef.org/documents/familiar-face-violence-lives-children