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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

DIGITAL RIGHTS AND CYBERCRIME AGAINST WOMEN: DOCTRINAL, COMPARATIVE AND EMPIRICAL REFLECTIONS

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

Digitization of daily life has altered the communication, meeting, work, and redress patterns of individuals to the extent that digital rights have become the cornerstone of the modern human rights discourse. Simultaneously, the growth of networked technologies has reinforced gendered cybercrime, such as online abuse, technology enabled sexual violence, image-based abuse and online sexual exploitation, which disproportionately impact women, girls and the gender diverse. These harms involve a broad range of basic rights privacy, freedom of expression, equality and non-discrimination, dignity, bodily autonomy, and the rights to justice and reveal endemic disparities between legal commitments on the book and the reality of the lives of the victim survivors. It is on this background that this paper will explore the digital rights of persons in the particular scenario of cybercrime against women with a doctrinal analysis, comparative legal approach, [1]and empirical evidence to assess existent protection and enforcement gaps, as well as, reform possibilities.

Conceptual and Legal Framework

The concept of digital rights is understood to be the translation and adaptation of the existing norms of human rights to the digital spaces, which are not entirely new from the very beginning.

[1] United Nations. (1948). Universal Declaration of Human Rights.

ISSN: 2582-6433

Human rights organizations all over the world have reiterated that human rights that are enjoyed by human beings in the offline world should also be secured on the internet, and notably the rights to freedom of expression, privacy, association and protection against violence and prejudice. In the case of women, these rights can be combined with the particular commitments declared in Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) and its General Recommendations on violence against women which demand that the States must undertake due diligence in addressing both offline and technology mediated gender-based violence .[2]

Cybercrime against women Cybercrime against women is crime that depends on or is enhanced by information and communication technologies and is directed against women due to their gender, sexuality or publicity, or has gender particular effects. These are online verbal abuse, doxing, threats of rape or other bodily harm, non-consensual creation or distribution of intimate image, online sexual exploitation, cyber stalking, and technology enabled trafficking and child sexual abuse content. Feminist scholarship has demonstrated that this kind of violence is not confined to specific incidents but is a result of structural gender hierarchies, misogyny, and rape culture, which is mirrored on digital space. Cybercrime against women is in this regard both a criminal law concern and a substantive equality concern, where states ought to address discriminatory social norms, institutional bias, and media frames and narratives and reformulate doctrinarism.

At the national level, jurisdiction attempts to cover cyber harms by enforcing a mixture of general criminal law (criminal intimidation, defamation, and obscenity) and specific cybercrime laws concerning unauthorized access, data interference and online content crimes. The Indian Penal Code, the communications Act and the Malicious Communications Act of the United Kingdom and the Cybercrime Prevention Act of the Philippines are examples of how various countries have tried to regulate online abuse and image based offences, with varying gender specificity. Nevertheless, the discontinuity of doctrine, high barriers to liability of criminal acts, and limited descriptions of harm routinely place women in situations with no solutions to justice, particularly when the mistreatment is chronic, compound, and entrenched in the social media systems of harassment.[3]

[2] United Nations. (1979). Convention on the Elimination of All Forms of Discrimination against Women (CEDAW).
[3] Committee on the Elimination of Discrimination against Women. (2017). General Recommendation No. 35 on gender-based violence against women.

ISSN: 2582-6433

Empirical Landscape of Online Abuse and Technology-Facilitated Sexual Violence

Empirical research is paramount in revealing the nature of how women are subjected to cybercrime, its experience, and how the victims-survivors can assess [4]the remedies they have been offered. The exploratory research conducted by the Internet Democracy Project on women and verbal online abuse in India records the variety of gendered abuse experienced by women who are publicly vocalized on social media like Twitter and blogs, this includes rape threats, sexually explicit insults, doxing, and attacks on family members. The paper underlines that these attacks do not concern the substantive points of women; instead, they are directed at the bodies and sexualities of women, which confirms the mother whore dichotomy and attempts to make a woman ashamed to remain silent. Online abuse therefore less concerns disagreement, rather it is the discipline of the women to engage in the communal discourse and thus prevent the freedom of expression and association.[5]

In the same study it is emphasized that anonymity and platform design enable abuse in several aspects. The behavior of perpetrators is based on anonymous or pseudonymous accounts to make threats and distribute degrading content on a large scale, and survivors tend to use anonymity as an effective defense mechanism to engage in online discourse without fear of retaliation in real life. Women use a continuum of non-legal methods that overlook and silence abusers, moderate comments, block and report accounts, find networks of solidarity and taking part in naming and shaming without necessarily realizing it, withdrawing to platforms, and with mental health effects such as anxiety and fear. Notably, trust in the lawlessness is highly diminished; respondents note bad experiences with law enforcement, such as trivialization of accusations, terrible knowledge of technology, and in some instances, 2nd victimization by victim-blaming interrogations.[6]

This picture is supplemented by Royal in her doctoral research on victim blaming, sexual violence and the media which demonstrates how media reporting on sexual violence influences the meaning of sexual violence among its victim's survivors and affects help seeking behavior. Her interviews with survivors and sexual violence support workers show that media discourses

[4] Council of Europe. (2011). Convention on preventing and combating violence against women and domestic violence (Istanbul Convention).
[5] Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).
[6] United Nations Human Rights Council. (2011). Guiding Principles on Business and Human Rights.

ISSN: 2582-6433

not only reproduce rape myths and subtle victim blaming, but also influence whether survivors will acknowledge their experiences as rape or not. Survivors project their own experiences onto highly publicized cases that fit the stereotypical scripts of real rape (stranger attacks, extreme physical violence, or idealized innocent victims) and downplay their own abuse when it comes to familiar attackers, coercion, but not force, or intoxication. This great fueler of non-identification has direct implications on the digital rights, since abused technology is often normalized or trivialized in mass and social media, and it is more difficult to refer to such abuses as violations that require redressing among women.[7]

Royal also demonstrates that the coverage of high-profile rape cases in the media can discourage as well as encourage reporting. Sensationalist reporting that emphasizes the credibility, sexual history, or lifestyle of victims or that emphasizes failures of the criminal justice system, can make survivors reluctant to cooperate with law enforcement in fear that they will be not believed or that they will be targeted with intrusive questions. Meanwhile, a legitimizing effect can be achieved by making sexual violence more visible and expose survivors as perceived in the context of the #MeToo movement, which means that delayed disclosure is valid and prompts some victims to seek support and justice even decades after abuse.[8] Viral hashtags, survivor led campaigns, and online solidarity networks have emerged as critical counter publics in the digital context that can speak, organize, and demand accountability by women through their digital rights to do so.

The Safer Kids PH action research of altering social norms surrounding online sexual abuse and online exploitation of children (OSAEC) in the Philippines builds upon empirical focus on the interplay between gender, childhood, and exploitation of children online. The paper has four significant social norms, which contribute to OSAEC, such as OSAEC is a taboo and unspeakable, it should not interfere with the private family affairs, victim blaming and stigma, and fixed gender roles and expectations that undermine the autonomy of women and children. People and communities tend to view OSAEC as an economic or personal problem and not a violation of rights; they are afraid of negative reputation and retaliation and do not want to report to anyone, even in the case when abuse is actively suspected in a community. These standards are acoustically consonant with the fact that these norms are common in other

[7] Internet Democracy Project. (2020). Let me speak: Online abuse and women's speech in India.
[8] Royal, S. (2019). Victim blaming, sexual violence and the media (Doctoral dissertation). University of Westminster.

ISSN: 2582-6433

jurisdictions, where online sexual exploitation is rampant in the context of poverty, patriarchal families, and ineffective child protection systems.[9]

Collectively, these empirical observations depict that cybercrime on women and girls is facilitated and reinforced by a set of technological affordances (anonymity, virality, content persistence), institutional failures (lack of legal definitions, insufficient resources in cybercrime units, inadequate training), and detrimental social practices (blame of victims, gender stereotypes, trivialization of online abuse). Consequently, although in some places through the form of digital rights, the rights of women to privacy, expression and body integrity are formally acknowledged, they are still conditional and fragile in their exercise.

Doctrinal Protections and Enforcement Gaps

Theoretically, the safeguarding of female digital rights is harnessed with the help of generic types of criminal laws which fail to fully reflect the gender nature and accumulative effects of online abuse. This is because a lot of criminal codes differentiate between threats, defamation, obscenity, and voyeurism, but they do not take into consideration the ways of coordinated, persistent harassment, which are just below the limits of each respective crime but together provide an atmosphere of fear and non-inclusion. E.g., image-based abuse can be charged under privacy, obscenity or data protection law in jurisdiction, with varying results and piecemeal solutions.[10]

The cybercrimes touch upon the Information Technology Act, the Indian Penal Code, the Protection of Children against Sexual offences Act, and, indirectly, the constitutional rights to equality and free speech in India. Where amendments have added offences like voyeurism and stalking and distribution of sexually explicit content, there are still major gaps in terms of addressing non-consent-based distribution of intimate images, deepfakes and gendered trolling that do not conform to the traditional obscene parameters. Furthermore, the law of the criminality is in many instances not enacted in cases of abuse exploitation on the online, the findings of the Internet Democracy Project of the unwillingness of the survivors of the online abuse to go to law enforcement are also indicative of the embedded patriarchal attitudes, the lack of technical skills, and the low priority the sufferings of the online victims have taken

[9] SaferKidsPH. (2022). Changing social norms on online sexual abuse and exploitation of children in the Philippines
[10] Government of India. (2000). Information Technology Act, 2000.

ISSN: 2582-6433

among the law enforcers.[11]

Law Lawmakers in the United Kingdom have constructed legal responses to online abuse based on offences under Malicious Communications Act, Communications Act, the Protection from Harassment Act, and more recent legislation of a revenge porn nature. Although some of these successful prosecutions have been possible, scholars believe that the emphasis on individualized malicious communications overshadows the context of misogynistic abuse and does not adequately consider platform responsibility to host and promote dangerous content. The examination of media coverage on sexual violence by Royal also indicates that criminal justice participants, such as juries, are not immune against rape myths and mythical stereotypes that are created by media, which are concerning the fair-trial provisions and equal protection when it comes to digital evidence and cases involving sexual violence enabled by technology.[12]

Another educative case is that of the Philippines. Its laws on the prevention of cybercrime, Anti-Violence against Women and their Children, and child-protection criminalize various kinds of sexual exploitations and abuse over the Internet, such as the creation and sharing of child sexual abuse content and live-stream exploitation. However, research of SaferKidsPH indicates that social norms of silence, non-interference and family honor are barriers to reporting and undermine enforcement despite legal structures seemingly strong on the paper. The members of the community might consider OSAEC as a means of living or a personal issue whereas women and children are stigmatized and victim-blamed when they report maltreatment. This disconnect between law in book and law in action points to the need to incorporate interventions of social norms in cybercrime and digital rights policy formation[13]

Comparative and International Normative Developments

On the comparative level, various jurisdictions and regional organizations have started to work out more explicit legal frameworks on the issue of online violence against women as one of human rights. The Istanbul Convention of the Council of Europe acknowledges that digital technologies can support psychological violence, stalking, sexual harassment and sexual violence and urges States to enact and otherwise address the issue by means of legislation and other actions in preventing, investigating and punishing such activity and providing support

[11] Government of India. (2012). Protection of Children from Sexual Offences Act
[12] United Kingdom. (1988). Malicious Communications Act.
[13] Philippines. (2012). Cybercrime Prevention Act of 2012.

ISSN: 2582-6433

services to their victims. The interpretation of the Budapest Convention on Cybercrime has also been adopted by the Council of Europe that highlights gender-sensitive practices and the necessity to combat online sexual exploitation and gender-based cyber-harassment.[14]

The UN Special Rapporteur on violence against women and girls and the UN Special Rapporteur on freedom of expression have both stated numerous times that technology facilitated gender-based violence is a danger not only to equality, but also to democratic participation. They have demanded the States to control the activities of the private firms, especially the social media to follow the UN Guiding Principles on Business and Human Rights, which states that businesses should exercise due diligence to prevent, mitigate and remedy the adverse human rights[15] effects caused by business, products and services. This means that a purely criminalization approach to the problem of digital rights cannot be effective; the platforms should be obligated to introduce transparent content moderation, quick reaction systems to gendered abuse, strong privacy and safety features, and easy ways to report as well as report on the content they carry.<|human|>It means that a criminalization of offenders is not sufficient to guarantee the digital rights; the platforms should be enforced with transparent content moderation, quick-reaction systems to gendered abuse, strong privacy and safety solutions, and available reporting systems, as well as mechanisms to report on the content available on A gradual shift towards image-based abuse, cyber stalking, and non-consent sharing of intimate images can also be found in comparative practice in the form of the Enhancing Online Safety Act in Australia, the Protecting Canadians from Online Crime Act in Canada, and other reforms in New Zealand and several European states. Critiques of such laws indicate that they address the gap in doctrines, but there is insufficient enforcement especially in marginalized women, who have intersecting axes of discrimination based on caste, race, class, sexuality, or disability. This puts an emphasis on the necessity of intersectional analysis when designing and implementing cybercrime frameworks.[16]

Discussion: Digital Rights, Structural Inequality and the Limits of Criminal Law

The above empirical and doctrinal analysis indicates three mutual dynamics which define the rights of women with respect to cybercrime in digital environment. To begin with, the existing gendered power relations and rape culture are embedded in and enhancing technology

[14] Canada. (2014). Protecting Canadians from Online Crime
[15] Australia. (2021). Online Safety Act 2021.
[16] CEDAW Committee. (2017). General recommendation No. 35 on gender-based violence against women. United Nations.

ISSN: 2582-6433

facilitated abuse. The example of victim blaming and media representations by Royal demonstrates how news discourses create hierarchies of victimhood, showing some to be more believable or worthy of pity than others, and often subtly suggesting that victims might have done more to [17]overcome harm by altering their behavior. Together with the abuse directed at women and their bodies and sexualities via the Internet that has been reported in the Internet Democracy Project study, these stories help to perpetuate the notion that women exist in the world including on the Internet, but only under the conditions and on the assumption that will continue to be subjected to moral judgment.

Second, formal legal systems have changed more quickly at the textual level of criminalization than at the institutional level and the social norms. Laws on stalking, harassment, and online sexual exploitation have been passed in India, the UK, the Philippines and numerous other states, but continue to be characterized by disbelief, lag time and lack of skill with digital evidence by law enforcers. Victim blaming, family privacy, community non-interference as emphasized in the SaferKidsPH research restrict reporting and subsequent cooperation with the authorities especially where it involves the perpetrator being a member of the family or intimate partner. The presence of crimes in the statute book, in these situations, does not equate to the successful enjoyment of the digital rights.

Policy and Law Reform Recommendations

The optimal approach to empower digital rights of women against cybercrime should be, therefore, multi-dimensional, involving the elucidation of doctrines,[18] institutional transformation, regulation of the platform, and change in social norms. It is firstly that legislatures should come up with clear gender sensitive definitions of technology facilitated gender based violence that can identify cumulative patterns of harm. It encompasses non-consensual creation and sharing of intimate images (including deepfakes), cyber stalking, doxing, and serious, repetitive online harassment, in terms that both directly engage perpetration and (knowing) facilitation by a third party. Online threats and abuse ought to be explicitly defined by law as gender-based violence even where there is no physical contact, which is in line with the international standards on psychological harm and coercive control.[19]

[17] Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. Wake Forest Law Review, 49, 345–391
[18] Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).
[19] European Institute for Gender Equality. (2017). Cyber violence against women and girls.

ISSN: 2582-6433

The criminal and procedural laws are to be restructured in order to be victim oriented in terms of investigation and prosecution. This involves dedicated cyber crime and gender desks in police departments, required training on digital evidence and gender bias, survivor centered interviewing policies, and protection against secondary victimization in the courtroom, including restrictions on intrusive questioning about sexual history and digital communications. The survivor should be able to find legal assistance and psychosocial support during the proceedings because the victim in this situation experiences the mental health consequences and traumatization reported in the scientific literature.

Policies that regulate platforms and internet intermediaries should be oriented towards human rights. Instead of outsourcing unaccountable censorship functions to privacy actors, states ought to move to due diligence-driven accountabilities that impose on platforms the duty to offer easy to use safety features and reporting procedures; respond swiftly to eliminate unlawful material like non-consenting intimate photos and OSAEC information; save proof of criminal investigations; and publish transparent information against gender-based mistreatment about content moderation. The regulation must also promote the inclusion of safety by design, including default privacy settings, mass messaging friction, and notifications against the sharing of intimate content without consent.

States and civil society should make the change in the social norms and digital literacy efforts that overcome victim blame, rape myths, and negative gender stereotypes. SaferKidsPH research demonstrates that the norms of taboo, non-interference and family honor can be solved with the help of community based conversations, school based intervention, and involvement of local leaders in case interventions are situation specific and participatory. The same strategies can be transferred to online violence against women more generally and it involves teaching about consent, responsible bystander, and respectful online use alongside survivor led narratives that humanize the harms of online violence and avoid attempts to normalize them.[20]

The digital rights approaches need to be intersectional, specifically focusing on those women who are the most vulnerable to cybercrime, such as journalists, human rights defenders, Dalit and Adivasi women and minority women, LGBTQ+ women and those with disabilities. Empirical studies have always indicated that women who hold visible positions in the public

[20] European Institute for Gender Equality. (2017). Cyber violence against women and girls.

ISSN: 2582-6433

space or threat to social structures of dominance receive more severe and organized online harassment, such as sexual violence threats. These groups should be prioritized in law, policy and platform responses so as to afford greater protection such as quick response, personalized safety advice, and strategic litigation assistance.

Lastly, additional empirical studies are necessary to base legal and policy changes on the realities on the ground of the affected people. The three articles reviewed in this paper show the importance of qualitative and survivor research in identifying how media discourse, social standards, and platform politics interact to determine digital rights. Subsequent research must involve longitudinal research to monitor the effects of new cybercrime laws, platform policies, and social norms interventions, disaggregated by gender, age, caste, class, race, ethnicity, sexuality and disability to determine whether the reforms actually increase women online rights exercising.[21]

Conclusion

Women and cybercrime is not a by-product of technology going bad but a continuation of the gender disparity and victim blame culture and an organizational breakdown into the online realm. Although the international and domestic legal frameworks are now increasingly recognizing the technology-facilitated gender based violence, the reviewed empirical evidence helps to prove that the digital rights of women are weak in observance, depending on the lack of proper doctrinal instruments, insufficient enforcement, and the social stigmatization of the survivors of the victims. The response based on rights needs to be further than criminalization to include platform accountability, victim-centric procedures, intersectional protection, and transformative social norms work.

With a focus on the experience of the survivors and the inclusion of digital rights as part of the substantive equality, states can develop legal and policy frameworks to address the direct harm of cybercrime and the structural aspects that support and permit it. It is not just to copy and paste analogue rights into the digital, but to reinvent legal structures, media cultures and technological architectures in the manner that would ensure that women and girls can enjoy a violence-free online space, where they can talk, organise and engage on equal terms.

[21] Royal, S. (2019). Victim blaming, sexual violence and the media (Doctoral dissertation, University of Westminster).Royal, S. (2019). Victim blaming, sexual violence and the media (Doctoral dissertation, University of Westminster).

ISSN: 2582-6433

REFERENCES

- Australia. (2021). Online Safety Act 2021 (Cth). Australian Government.https://www.legislation.gov.au/Details/C2021A00037
- Canada. (2014). Protecting Canadians from Online Crime Act (S.C. 2014, c. 31).https://laws-lois.justice.gc.ca/eng/AnnualStatutes/2014_31/
- CEDAW Committee. (2017). General recommendation No. 35 on gender-based violence against women. United Nations.https://undocs.org/CEDAW/C/GC/35
- Citron, D. K. (2014). Hate crimes in cyberspace. Harvard University Press.https://www.hup.harvard.edu/catalog.php?isbn=9780674972353
- Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. Wake Forest Law Review, 49, 345–391.https://scholarship.law.ufl.edu/facultypub/244
- Council of Europe. (2001). Convention on Cybercrime (Budapest Convention).https://www.coe.int/en/web/cybercrime/the-budapest-convention
- Council of Europe. (2011). Istanbul Convention: Convention on preventing and combating violence against women and domestic violence.https://www.coe.int/en/web/istanbul-convention
- European Institute for Gender Equality. (2017). Cyber violence against women and girls.https://eige.europa.eu/publications/cyber-violence-against-women-and-girls
- Government of India. (1860). Indian Penal Code.https://legislative.gov.in/actsofparliamentfromtheyear/indian-penal-code
- Government of India. (2000). Information Technology Act, 2000.https://legislative.gov.in/actsofparliamentfromtheyear/information-technology-act-2000
- Government of India. (2012). Protection of Children from Sexual Offences Act.https://legislative.gov.in/actsofparliamentfromtheyear/protection-children-against-sexual-offences-act-2012
- Henry, N., & Powell, A. (2015). Embodied harms: Gender, shame, and technology-facilitated sexual violence. Violence Against Women, 21(6), 758–779.https://journals.sagepub.com/doi/10.1177/1077801215576581
- Internet Democracy Project. (2020). Let me speak: Online abuse and women's speech in India.https://internetdemocracy.in/2020/11/let-me-speak/
- Jane, E. A. (2017). Misogyny online: A short (and brutish) history. SAGE.https://us.sagepub.com/en-us/nam/misogyny-online/book245110

ISSN: 2582-6433

- Mantilla, K. (2015). Gendertrolling: How misogyny went viral. Praeger.https://www.abc-clio.com/ABC-CLIOCorporate/product.aspx?pc=A4764C
- Philippines.(2012).CybercrimePreventionActof2012.https://lawphil.net/statutes/repacts/ra2012/ra_10175_2012.html
- Royal, S. (2019). Victim blaming, sexual violence and the media (Doctoral dissertation). UniversityofWestminster.https://westminsterresearch.westminster.ac.uk/item/q2v42/victim-blaming-sexual-violence-and-the-media
- SaferKidsPH. (2022). Research on online sexual abuse and exploitation of children.https://saferkids.ph/wp-content/uploads/2022/05/SaferKidsPH-Research-Report.pdf
- UN General Assembly. (1948). Universal Declaration of Human Rights.https://www.un.org/en/about-us/universal-declaration-of-human-rights
- UN General Assembly. (1979). Convention on the Elimination of All Forms of Discrimination against Women.https://www.un.org/womenwatch/daw/cedaw/
- UN Human Rights Council. (2011). Guiding Principles on Business and Human Rights.https://www.ohchr.org/en/professionalinterest/pages/businesshr.aspx
- UN Human Rights Council. (2012). The promotion, protection, and enjoyment of human rights on the Internet.https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/20/L.13
- UN Special Rapporteur on violence against women. (2018). Report on online violence againstwomenandgirls.https://www.ohchr.org/en/statements/2018/11/online-violence-against-women-and-girls
- UN Women. (2020). Online and ICT-facilitated violence against women and girls during COVID-19.https://www.unwomen.org/en/digital-library/publications/2020/09/report-on-online-and-ict-facilitated-violence-against-women-and-girls
- Woodlock, D. (2017). The abuse of technology in domestic violence. Violence Against Women, 23(5), 584–602.https://journals.sagepub.com/doi/10.1177/1077801216654573
- Wright, M. F. (2018). Cyber victimization and mental health among women. Journal of InterpersonalViolence,33(17)2737–2756.https://journals.sagepub.com/doi/10.1177/0886260516659658

ISSN: 2582-6433

- Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs. https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/
- United Nations. (2021). Report on digital rights and gender-based online violence.https://digitallibrary.un.org/record/395780
- Amnesty International. (2018). Toxic Twitter: A toxic place for women. https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1
- World Bank. (2021). Voices and Votes: Gender equality in the digital age.https://documents.worldbank.org/en/publication/documents-reports/documentdetail/113011632967763613/voices-and-votes-gender-equality-in-the-digital-age