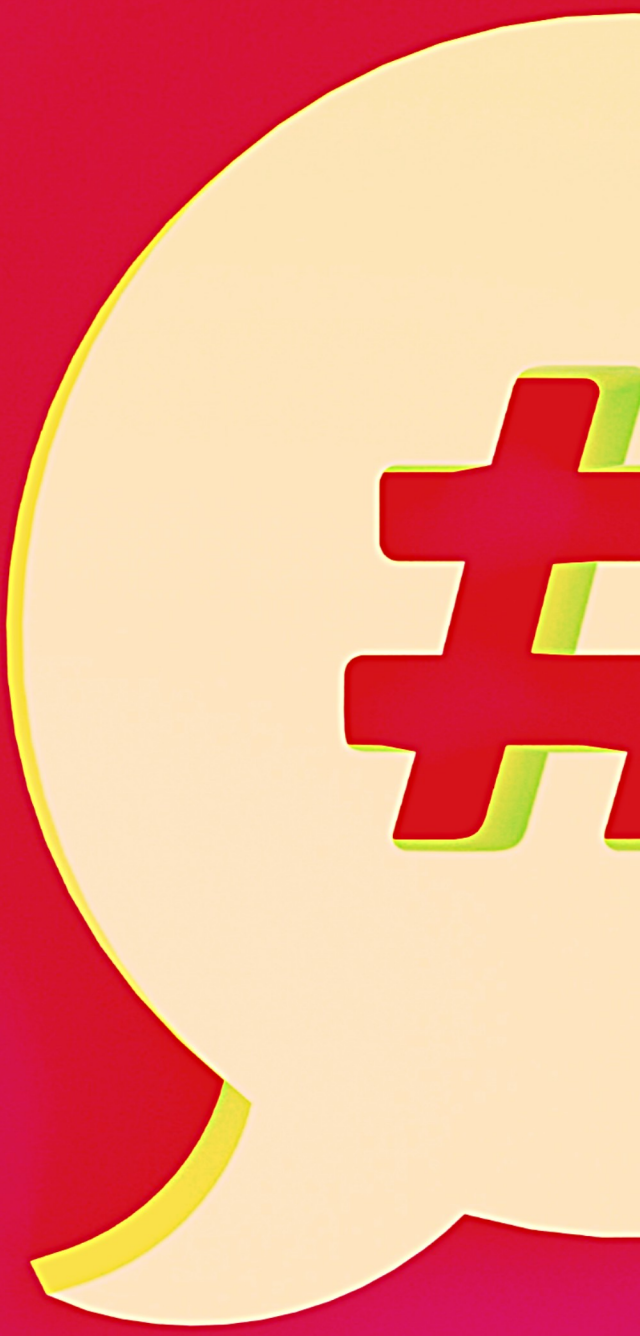
Rethinking Legal-Institutional Approaches to Sexist Hate Speech in India

Role of the Law in Combating Online Misogyny, Hate Speech and Violence Against Women and Girls

N. S. Nappinai



IT for Change
February 2021

Role of the Law in Combating Online Misogyny, Hate Speech and Violence Against Women and Girls

N. S. Nappinai

N. S. Nappinai is an advocate at the Supreme Court of India & the Founder of Cyber Saathi.

This paper is part of a series under IT for Change's project, Recognize, Resist, Remedy: Combating Sexist Hate Speech Online. The series, titled Rethinking Legal-Institutional Approaches to Sexist Hate Speech in India, aims to create a space for civil society actors to proactively engage in the remaking of online governance, bringing together inputs from legal scholars, practitioners, and activists. The papers reflect upon the issue of online sexism and misogyny, proposing recommendations for appropriate legal-institutional responses. The series is funded by EdelGive Foundation, India and International Development Research Centre, Canada.

February, 2021

Conceptualisation

Anita Gurumurthy, Nandini Chami, Bhavna Jha

Editors

Anita Gurumurthy, Bhavna Jha

Editorial Support

Amay Korjan, Ankita Aggarwal, Sneha Bhagwat, Tanvi Kanchan

Design and Layout

Sneha Bhagwat

N. S. Nappinai

Role of the Law in Combating Online Misogyny, Hate Speech and Violence Against Women and Girls

Introduction

Physical violence against women has been normalised through rape culture, victim blaming, and self-imposed restraint by victims over their own conduct. As the continuum of violence against women and girls extends seamlessly to online spaces, such normalisation is now evident in virtual domains as well. This paper explores the increasingly aggravated forms of cyber violence against women and girls (VAWG), the correlation between physical and cyber misogyny, the efficacy of existing laws in combating the issue, the effect of categorising online misogyny and gender-based hate speech as 'hate crimes', the steps and solutions India could explore by reviewing its Information and Communication Technology (ICT) and criminal laws, and the need for international cooperation to evolve more effective and harmonised laws to combat the problem. The paper also advocates for effective enforcement of laws, existing or additional, for sustainable impact in curbing cyber VAWG.

1. Misogyny Through the Ages

"Demure women who do not look a man in the eye don't get assaulted."

"Shaming a man; laughing at a leader; being sarcastic to a man; being scornful – these are unbecoming for a woman and are bound to lead to disastrous consequences."

These familiar sounding statements come from the Mahabharata,[1] one of India's great epics. The story focuses on the internecine rivalry among warring factions in a dynasty, and places the public assault, disrobing, sexual violence, and dishonouring of a queen at the heart of the conflict. While the justifications for violating a woman's dignity may have changed over the years, victim blaming – including judgements about her conduct or appearance, amongst other 'mistakes' continues to be a common thread, reflecting a deep-rooted misogyny in everyday cultures.

Physical violence against women and girls has seamlessly extended into online spaces, in a reproduction of what Liz Kelly refers to as the "continuum of sexual violence".[2] Aggravated forms of online violence and victim blaming[3] continue unabated.[4] The reasons for toxicity online remains eerily similar over the ages, i.e., of victim blaming and shaming. Perpetrators erroneously assuming that online domains provide them with a veil of protection has resulted in "toxic disinhibition"[5] and consequent intensification of violence online with far worse consequences for victims, who face the risk of harmful and derogatory content being disseminated to millions without any territorial restraint. A study commissioned by the European Parliament's Policy Department for Citizen's Rights and Constitutional Affairs[6] points to a normalisation of online violence similar to offline crimes. Cases handled by the author[7] and reported cases[8] also demonstrate the reality of victim blaming.[9] Women who face cyber VAWG are often advised to 'not feed the troll', 'change their privacy settings' and to 'go offline for a while'. These narratives are repeated not only by parents and other authority figures, but also by law enforcement officials, which subjects victims to moralistic and judgmental inquisitions. Law enforcement and in some instances courts believe that online violence is virtual,

---

[1] Rajagopalachari, C. (1951). Mahabharata. Bombay: Bharatiya Vidya Bhavan. The authorship of the original epic is attributed to Krishna Dwaipayan Vyasa or 'Vedavyasa', a rishi. One of the earliest English renditions was by C. Rajagopalachari, former Chief Minister of Tamil Nadu, India.

[2] Kelly, L. (1987) The Continuum of Sexual Violence. In: Hanmer J., Maynard M. (eds) Women, Violence and Social Control. Explorations in Sociology (British Sociological Association Conference Volume series). Palgrave Macmillan, London.

[3] Ryan, W. (1970). Blaming the Victim. Knopf Doubleday Publishing Group, 2010.

[4] Nappinai. N. S. (2020). "Rethinking Social Media – Through the Prism of Freedoms, Liberties & Victim Rights" in "Essays & Reminiscences – Festschrift Book for Nani Palkivala". LexisNexis.

[5] Suler, J. 2005. The online disinhibition effect. International Journal of Applied Psychoanalytic Studies 2(2):184–188.

[6] https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

[7] References cases personally handled by the author, who inter alia specialises in handling cybercrime cases.

[8] Online Harassment Report. PEW Research Center – Internet & Technology. Available at: https://www.pewresearch.org/internet/2014/10/22/part-1-experiencing-online-harassment/

[9] Rajendran, A. (2019). Cyber Crimes and Victim Shaming in India. Available at: https://www.researchgate.net/publication/330753191_Cyber_Crimes_and_Victim_shaming_in_India_Cyber_Crimes_and_Victim_shaming_in_India

and that victims just have to turn off their computer and walk away, an understanding that is far removed reality.[10]

This propensity to blame the victim also results in 'remedies' that are oriented towards 'educating' victims and advising them to modify their conduct instead of addressing the root cause of the violence. The truisms that William Ryan identified in his pathbreaking work 'Blame the Victim' in 1970 of blaming "the powerless for their powerlessness", has contemporary applicability. It is most evident in awareness programs that focus on 'educating victims' and teaching them to stay safe, instead of warning potential criminals of the consequences of crimes against women.

Patriarchy and misogyny manifest in multiple facets, not just in India, but across the world and modus of online VAWG is demonstrably similar. Online VAWG is identified as an intensifying harm but solutions that effectively protect victims' rights appear elusive.

2. The Digital as a Medium for Misogyny, Hate Speech, and Crime

a. Popular Media and Its Impact on Gendered Crimes

Misogyny is ubiquitous in popular culture. From advertising to movies, sexist narratives continue to hold fort. Popular advertising campaigns that objectify women and use stereotypical taglines like "It's not for girls" to advertise chocolate bars for 'men',[11] merely reinforce male hegemony and justify bigotry. Movies are not far behind in reinforcing chauvinistic narratives.

This reiteration of misogynistic ideas through popular media adversely affects psycho-social behaviour. A study about behavioural changes that result from watching aggressive pornographic content indicates increased aggression towards women without impacting male targets of aggression.[12] Unsurprisingly, with misogyny shaping social conduct, alternative narratives get buried and 'feminism' becomes a tainted and unpopular term.

---

[10] Nappinai. N. S. (2017). Tackling Women's Digital Freedoms and Unfreedoms Online – Through Law & Technology. IT For Change. https://itforchange.net/e-vaw/wp-content/uploads/2017/12/OPinion-piece-II.pdf

[11] https://www.thedrum.com/news/2017/07/20/another-era-the-decades-most-sexist-ads-ft-protein-world-carls-jr-lynx-and-more

[12] Donnerstein, E., & Berkowitz, L. (1981). Victim reactions in aggressive erotic films as a factor in violence against women. Journal of Personality and Social Psychology, 41(4), 710–724.

b. Online Targeted Violence Against Women

Contrary to the assumption that the cyber domain would facilitate unfettered freedoms, the ever-widening reach of technology has only increased its potential to cause deeper harm with women facing the worst effects of online hate.[13] In 2015, a UNESCO report, 'Cybercrime Against Women & Girls – A Worldwide Wake Up Call'[14] stated that 73 percent of women have already been exposed to or have experienced some form of online violence. Amnesty International's 2018 report[15] affirms this trend with respect to social media-based offences against women.

Besides, physical and cyber violence often overlap and intersect. A survey of violence against women conducted by the European Union Agency for Fundamental Rights found that 70-77 percent of victims of cyber stalking or online sexual harassment victims had also experienced sexual harassment or violence from intimate partners.[16] Objectification, trolling through sexual innuendo, physical harm, doxxing and exposés of intimate images of women without consent, verbal abuse through threats of physical harm, rape, gang rape, name-calling, and body-shaming are among an ever expanding list of online crimes against women carried out with increasing vigour and impunity.[17]

c. Misogyny Online – Crime or Hate Crime?

On June 1, 2020, as the academic year commenced in India, largely online on account of the Covid-19 pandemic, a Kerala educator suddenly found herself the subject of the viral 'blue sari teacher' memes, and was viciously trolled, bullied and vilified[18] following pre-recorded lectures. Her trolling was replete with sexual innuendo and objectification.[19] But this conduct is just the tip of the proverbial iceberg.

---

[13] *Ibid*. 10.

[14] https://en.unesco.org/sites/default/files/genderreport2015final.pdf

[15] Amnesty International (2018), Toxic Twitter, a toxic place for women, available at https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

[16] European Union Agency for Fundamental Rights (FRA), 2014, "Violence against women: an EU – wide survey". Available at: https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

[17] *Ibid*. 20.

[18] https://www.newindianexpress.com/states/kerala/2020/jun/03/this-english-teacher-is-an-instant-hit-for-her-online-lessons-but-trolled-mercilessly-2151427.html

[19] https://feminisminindia.com/2020/06/16/blue-saree-teacher-case-kerala-sexualisation-policing-women

The last decade has seen a disturbing trend of rape and gang rape videos being uploaded on social media platforms. When victims' repeated attempts to take down such content failed, the NGO Prajwala addressed a letter to the Chief Justice of India, prompting the Supreme Court to take *suo moto* cognizance of the issue in 2015[20] (referred to hereunder as *Prajwala v. UOI*).[21]

In 2013, author and activist Kavita Krishnan faced rape and gang rape threats during an online chat session from a participant, who used the handle "rapist".[22] In 2020, MS Dhoni's 5-year-old daughter received rape threats[23] after his team lost a cricket match. The alleged perpetrator was a teenager.[24] From 2013 to 2020, the only difference is the reduction in the age of the demographic of both the perpetrator and the victim.

> In most cases of online trolling and violent speech, the perpetrators may be total strangers; there is no direct provocation by the victims and apart from a perceived sense of affront or thrill-seeking there may not really be any grounds for these attacks.

These examples of cyber VAW would by themselves amount to crimes. However, hate speech is an aggravated form of crime that lends itself to greater punitive action. Megan Sullaway[25] uses legal definitions under US statutes[26] to describe hate crimes as crimes in which the victim is targeted due to "actual or perceived race, color, religion, disability, sexual orientation, or national origin". This definition follows the trend that has emerged from hate crime legislations across several jurisdictions. Notably, none of these legislations list gender as a category. Boyd, Berk, and Hamner[27]

---

[20] Suo Motu Criminal Writ Petition No. 3 / 2015.

[21] The author is Amicus Curiae in this case before the Supreme Court and also part of the Government Committee appointed thereunder and hence references herein are only to those facts and details available in public domain through orders of the Hon'ble Supreme Court of India.

[22] https://www.firstpost.com/tech/news-analysis/rape-threat-to-kavita-krishnan-does-the-internet-belong-to-the-cyber-bully-2-3624599.html

[23] https://www.deccanherald.com/cricket/ipl/m-s-dhonis-5-year-old-daughter-ziva-gets-rape-threats-after-csk-loses-match-to-kkr-899986.html

[24] https://www.timesnownews.com/sports/cricket/article/16-year-old-arrested-in-gujarat-for-issuing-rape-threats-to-ms-dhonis-daughter/665783

[25] Sullaway, M. (2004). Psychological perspective on hate crime laws. Psychology, Public Policy, and Law, 10, 250–292.

[26] Such as the Hate Crime Statistics Act, 1990, which defines "hate crimes" as an offence "that manifests evidence of prejudice based on race, religion, disability, sexual orientation, or ethnicity".

[27] Boyd, E. A., Berk, R. A., & Hamner, K. M. (1996). "Motivated by hatred or prejudice": Categorization of hate-motivated crimes in two police divisions. Law & Society Review, 30, 819–850. Cal. Penal Code § 1170.75 & § 190.

list the following criteria used by police officers to identify a hate crime: "no provocation by the victim, a specific target, no prior encounter between victims and perpetrator, and accompanying derogatory remarks."

Even a cursory look at trending online gendered hate speech would demonstrate that each one of Boyd, Berk, and Hamner's criteria is relevant in this regard. In most cases of online trolling and violent speech, the perpetrators may be total strangers, there is no direct provocation by the victims, and, apart from a perceived sense of affront or thrill-seeking, there may not really be any grounds for these attacks.

Hate crime, being a contextual issue, raises several concerns about categorisation, and may create further complications when applied to gendered crimes. This is not only because of the nature of the crime but also because intent and import play a significant role in identifying a hate crime. McPhail[28] argues that the "socialization of sex roles, gender stereotypes and expectations, the historic legacy of minimizing violence against women, and the male justification of rape all play a part in not recognizing violence against women as a hate crime." Green, Abelson, and Garnett[29] suggest that the uncertainties caused by changing public roles, including gender roles, lead to hate crimes.

> Considering that the very basis for misogyny is gendered prejudice, hatred, and contempt for a specific category of people, that is, women, it could be argued that the elements of a typical hate crime are evidently present.

The causation for hate crimes is not only based on, or identified through, crimes targeting specific groups. Crimes motivated by diverse intentions, from group identity, a common intention or purpose (which could include mere thrill-seeking), threat to established normative behaviour, or fear of the loss of privileges, are also considered hate crimes.[30]

When cyber VAWG is considered from this broader perspective – threats to the status quo as the basis for crimes – each of the above instances could be categorised as a hate crime. While gender-based crimes were initially excluded from the category of hate crimes based on the specific

---

[28] McPhail, B. (2002) 'Gender-bias Hate Crime: A Review', Trauma, Violence and Abuse 3(2): 125–45.

[29] Green, D. P., Abelson, R. P., & Garnett, M. (1999). The distinctive political views of hate crime perpetrators and white supremacists. In D. Prentice & D. Miller (Eds.), Cultural divides: Understanding and overcoming group conflict (pp. 429–464). New York: Sage.

[30] McDevitt, J., Levin, J., & Bennett, S. (2002). Hate crime offenders: An expanded typology. Journal of Social Issues, 58, 303–318.

definition of group identity-driven crimes against outsiders, its subsequent inclusion is founded on tenuous acceptance, which has also resulted in weak implementation.[31]

Considering that the very basis for misogyny is gendered prejudice, hatred, and contempt for a specific category of people, that is, women, it could be argued that the elements of a typical hate crime such as groupism, hatred towards a specified category, and violence against targeted groups, are evidently present.

Escalating the categorisation of a crime to a hate crime is predicated on it being "motivated by bias toward individuals or groups based on particular status characteristics such as race, religion, ancestry, sexual orientation, or gender".[32] Drawing on this, Bleich[33] concludes that "[m]ost of these laws boost punishment for underlying crimes (such as assault, vandalism or intimidation) carried out because of biased motives which the state deems particularly opprobrious."

The US, with its strong free speech doctrine, opposed restraints, even on racist hate speech. However, in *Wisconsin v. Mitchell,*[34] the US Supreme Court drew a fine line by stating that the "Wisconsin statute against aggravated battery motivated by racism in fact penalised the conduct of the perpetrator, not his thought or expression"[35]. This judgement was followed by a plethora of hate crime statutes in the US, at both Federal and State levels, including the 'Violent Crime Control and Law Enforcement Act of 1994',[36] which includes gender as a specific category for determining hate crime and consequent enhanced penalties.

Applying the above delineation to hate speech online may pose further hurdles since the lines separating thought, expression, and conduct merge substantially. However, cyber bullying or online sexual hate crimes, like the ones dealt with in *Prajwala v. UOI,* are not mere expressions of thought but of actuation of conduct that "cause greater societal harm and injury to the individual and community victims".[37]

---

[31] McPhail, B. (2002) 'Gender-bias Hate Crime: A Review', Trauma, Violence and Abuse 3(2): 125–45.

[32] Jenness, V. and Grattet, R. (2001) Making Hate a Crime: From Social Movement to Law Enforcement. New York: Russell Sage Foundation.

[33] Bleich, Erik. 2011. "The Rise of Hate Speech and Hate Crime Laws in Liberal Democracies." Journal of Ethnic and Migration Studies 37(6):917–934.

[34] 508 US 476 (1993).

[35] Bleich, Erik. 2011. "The Rise of Hate Speech and Hate Crime Laws in Liberal Democracies." Journal of Ethnic and Migration Studies 37(6):917–934.

[36] Public Law 103-322, H.R. 3355, which makes it hate crime when a victim is intentionally selected "because of the actual or perceived race, color, religion, national origin, ethnicity, gender, disability or sexual orientation of any person"; Also see 'Hate Crimes Sentencing Enhancement Act, 1994".

[37] Lawrence, F.M. (1999) Punishing Hate: Bias Crimes under American Law. Cambridge: Harvard University Press.

This greater societal harm manifests online through conduct that not only amounts to cyber bullying, cyber stalking, or uploading of rape and gang rape imagery, but also deviant hate conduct that devalues victims based on their group identity – in this instance, gender. As Hawdon et al.[38] explain, "Hate materials do not attack individuals in isolation; instead, these materials, which include text, videos, photos, games, and other modes of communication, express hatred or degrading attitudes toward a collective."

Categorising certain forms of cyber violence – such as gendered hate speech, uploading of violent and/or sexual content against women, and the use of the online space for intimidatory purposes – as hate crimes is therefore necessary and feasible. Bleich captures the urgent need for legislations to specifically include gender-based hate crimes: "Legislation has a strong declarative effect when it is enacted: in these cases, it asserts that certain expressions are deemed unacceptable by the country as a whole and reassures vulnerable groups that their interests and identities are considered worthy of national acknowledgement."[39]

d. Online Crimes – Physical and Economic Harm

The myth that online crimes are not as harmful as physical attacks has been countered in recent studies, including the 2020 Child Relief and You (CRY) report[40] and the EU Parliament's 2018 study.[41] There also appears to be a misconception regarding the extent of harm caused by online crimes, and a tendency to ignore their economic costs. Online platforms are not only a means of communication or connection but also a site of conducting business for many. Social media platforms have evolved into virtual marketplaces, and it is not feasible for a victim of online violence – or any person for that matter – to stay away from such platforms. When a person's online presence is disrupted through violent acts, it has the same, if not an aggravated effect on the victim as offline attacks. Online violence creates "a genuine fear of violence with all its attendant psychological, emotional, economic, and social disruptions".[42]

Hence, while deciding whether the law ought to treat online hate speech as a crime or hate crime, the physical, psychological, and financial impact of such crimes ought to be accounted for.

---

[38] James Hawdon, Atte Oksanen, and Pekka Räsänen, (2017). "Exposure to Online Hate in Four Nations: A Cross-National Consideration," Deviant Behaviour 38, no. 3. 254–66.

[39] Bleich, Erik. 2011. "The Rise of Hate Speech and Hate Crime Laws in Liberal Democracies." Journal of Ethnic and Migration Studies 37(6):917–934.

[40] https://www.cry.org/wp-content/uploads/2020/02/Online-Safety-and-Internet-Addiction-p.pdf

[41] https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

[42] https://www.theguardian.com/law/2014/nov/30/threat-kill-joke-art-supreme-court-online-facebook-anthony-elonis

3. The Law as a Protector

a. How Effective is the Law?

The process of legal reform will be ineffectual unless existing laws and their enforcement are appropriately evaluated. Law and enforcement play key roles in ensuring the safety and protection of citizens through retributive punishments and, more significantly, by acting as deterrents.[43] However, effective enforcement of the existing laws is necessary to achieve this, since laws by themselves do not suffice.

Criminal justice is contingent on sanctions as well as the implementation of such sanctions. As such, accessing enforcement must be easy, delivery of justice must be expedient, and punishments or outcome must be commensurate with the offence committed.

The facts resulting in *Prajwala v. UOI*[44] i.e., of uploading of rape and gang rape videos online, highlights the impunity with which the evidence for crimes like rape and gang rape is recorded and shared by perpetrators online. It demonstrates perpetrators' confidence that they will not be caught, while foregrounding the reasons why victims lack faith in the existing system. Neither of these is conducive to maintaining a social structure, least of all a democracy.[45]

b. Will Adding More Laws or Provisions Help?

Merely adding provisions to existing laws will not help improve protections for victims. The outcome of the Nirbhaya case is a classic example. The gravity of the offence in the case culminated in wide-ranging action, starting with the appointment of the Justice Verma Committee on December 23, 2012.[46] The Committee's report led to an overhaul of India's criminal legislations through The Criminal Law (Amendment) Act, 2013, with significant revisions to the rape laws, and criminalisation of sexual harassment, voyeurism, and stalking. However, due to their ineffective enforcement,[47] these amendments have not been able to sufficiently deter crime against women or safeguard victims' rights.

---

[43] Nappinai N. S. (2017). Technology Laws Decoded. Published by LexisNexis.

[44] *Ibid*. 20.

[45] Nappinai N. S. (2019). Indian women must get justice and it must be timely. But vigilantism is anathema to both justice and democracy. Times of India. Available at: https://timesofindia.indiatimes.com/blogs/toi-edit-page/indian-women-must-get-justice-and-it-must-be-timely-but-vigilantism-is-anathema-to-both-justice-and-democracy/

[46] https://timesofindia.indiatimes.com/realtime/justice_js_verma_committee_report.pdf

[47] https://ncrb.gov.in/sites/default/files/CII%202019%20Volume%201.pdf

One addition that seems to be a dead letter from its inception is Section 166A of the Indian Penal Code (IPC), which seeks to criminalise the failure of a public servant to perform his duties in certain instances, including the failure to register complaints of rape and other specified offences. Despite the inclusion of this explicit provision that makes the registration of first information reports (FIRs) mandatory, there have been reports of the police refusing to register rape cases as recently as January 10, 2021.[48] The failure to prevent law enforcement officials from refusing to register FIRs reflects not only on the salutary nature of this addition but also on the failure of its draftsperson to provide explicit mechanisms that make this addition more than just a paper tiger. While amending criminal laws as well as cyber security laws, therefore, it is necessary to also develop effective means for their implementation.

c. Trends in International Human Rights Frameworks

The United Nations Special Rapporteur's Report on Violence Against Women, presented to the UN Human Rights Council in June 2018,[49] defines online violence against women as "gender-based violence against women that is committed, assisted, or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately".

The Convention on Cybercrime[50] or the Budapest Convention, which is presently adopted by about 64 countries, does not address cyber VAWG specifically, although its general provisions could benefit victims of cyber VAWG also. The 2003 Additional Protocol to the Convention on Cybercrime[51], despite advocating for specific laws to combat racism and xenophobia, does not address gender as a basis for hate speech. In 2018, a further Additional Protocol to the Convention on Cybercrime was introduced for consideration. This draft not only defines online hate speech but also sexist hate speech online as "expressions which spread, incite, promote, or justify hatred based on sex".

Increasing violence against women online has led multiple jurisdictions to review their laws. India is not a signatory to the Budapest Convention, but with increasing cyber threats, it appears to be

---

[48] https://timesofindia.indiatimes.com/city/bareilly/minor-sisters-alleged-rape-circumstantial-evidence-non-indicative-of-rape-says-co/articleshow/80191369.cms

[49] Human Rights Council (2018), thirty-eighth session, 18 June – 6 July 2018, "Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective", available at https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx

[50] The first Convention on cybercrime, also referred to as the Budapest Convention, effective November 23, 2001. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[51] January 28, 2003. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008160f

relaxing its resistance to review this position.[52] Given the jurisdictional limitations of municipal laws, and the cross-jurisdictional reach of the internet and social media platforms, it is imperative that mutually-mediated international laws be developed to combat cyber VAWG.[53]

4. Existing Laws and Remedies in India to Combat Online VAWG

a. India – IT Act and IPC

The National Crime Records Bureau (NCRB) 2019 report shows a substantial increase in cybercrimes, but this has mostly been attributed to a rise in financial crimes relating to fraud (56 percent or 12,213 of 21,796 cases). Sexual exploitation (6.7 percent), causing disrepute (4.6 percent), pranks, and personal revenge constitute the rest of the increased criminal activity. The NCRB statistics, however, may not be representative of the real threat of the cyber domain in India, where 70 percent of the population has internet connectivity. It may, instead, be a reflection of the trust deficit in the systemic remedies that dissuades victims from seeking legal redress.

Online misogyny is currently covered by the Information Technology Act, 2000 (as amended) (IT Act) and the Indian Penal Code, 1860 (IPC). The IT Act covers the violation of privacy (Section 66E); publishing and transmission of obscene, sexually explicit acts and child pornography or Child Sexual Abuse Material (Sections 67, 67A, and 67B); identity theft (Section 66C); and cheating by personation (Section 66D). Each of these sections, in some form, is applicable to offences such as 'revenge porn' or cyber extortion, and cases such as in *Prajwala v. UOI*. Pursuant to the Criminal Law Amendments of 2013, provisions for voyeurism (354C), stalking (354D), and violence with the intent to disrobe a woman (354B) were introduced. These provisions address online violence against women. Section 66A of the IT Act, which dealt *inter alia* with the dissemination of offensive messages online, was struck down by the Supreme Court in *Shreya Singhal v. Union of India*[54] in the light of its rampant abuse. The provision was also open-ended and ambiguous.

---

[52] https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/

[53] Nappinai. N. S. (2017). Technology Laws Decoded. Chapter 7: Broken Windows in Cyberspace. The Need for International Enforcement Mechanisms. LexisNexis.

[54] (2015) 5 SCC 1.

b. Enforcement Issues

Presently, online misogyny is broadly covered under general and special laws in India and not recognised as a hate crime. Even with this broad categorisation, there has not been much success in either prosecutions or convictions. KPMG's Cybercrime Survey Report (2014)[55] sets out India's abysmal cyber-crime reporting, registration, and conviction statistics. With just four people being convicted as of August 2009, and a 10 percent reporting rate for cyber crimes, India is certainly not topping the enforcement index.[56] It is not clear how enhanced recognition as a hate crime would, on its own, improve enforcement.

c. Takedowns and Intermediaries

Social media platforms came into their own alongside sweetheart deals of 'safe harbour' under the wide protection of Section 230 of the US Communications Decency Act (CDA), 1996.[57] This provision, which is referred to as the "26-word immunity" grants extensive protections to intermediaries/social media platforms. However, such protections were predicated on the service providers being 'dumb pipes' and not having much control over the content hosted online.

India's equivalent – Section 79 of the IT Act – was not as sweet a deal for intermediaries since it placed the onus on the intermediaries to prove their innocence. However, amendments to the Section in December 2008 changed this substantially and granted wide exemptions. Under the present Section 79 of the IT Act, intermediaries – from Internet Service Providers to social media platforms – are exempted from liability if their functionality is limited to "providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted" or where the intermediary does not "(i) initiate the transmission; (ii) select the receiver of the transmission; and (iii) select or modify the information contained in the transmission". They are also required to observe due diligence and comply with the guidelines of the central government.

Section 79(3)(b) also mandates intermediaries to remove unlawful content upon having knowledge of it, or being notified about it by a government agency. Failure to comply, through expeditious takedowns, could result in negating the protective shield of Section 79(1) of the IT Act. Pursuant to the powers vested under this provision and the IT Act, the Information Technology (Intermediaries

---

[55] KPMG (2014). Cybercrime survey report 2014. https://assets.kpmg/content/dam/kpmg/pdf/2014/07/KPMG_Cyber_Crime_survey_report_2014.pdf

[56] Kshetri, N. (2016). "Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future" Crime, Law and Social Change, 66 (3), 313 – 338.

[57] 47 U.S.C. § 230, of Communications Decency Act of 1996.

guidelines) Rules, 2011 (Intermediary Rules) were notified. These rules mandate that intermediaries must take down unlawful content within 36 hours of obtaining knowledge about any such content.

The Supreme Court of India in *Shreya Singhal v. UOI*[58] dealt with the legality of the above provision (Section 79, IT Act) and the Intermediary Rules (Rule 3(4) in particular), and upheld takedowns by intermediaries pursuant to acquiring knowledge of unlawful content either through a government notice or court order. However, the Supreme Court struck down the portion that mandated takedowns pursuant to notice from users since it could stifle free speech.

One of the unintended consequences of the above judgment, which focused primarily on protecting free speech, is the increased delay in the takedown of violent content against women from online platforms. Presently, the situation with respect to intermediary liability and protection is as follows:

- Subject to intermediaries complying with the conditions mandated under Sections 79(2) and 79(3) of the IT Act, the exemption from liability continues;
- With respect to both, Section 79(3)(b) of the IT Act and Rule 3(4) of the Intermediary Rules, the Supreme Court limited the duty of intermediaries to act "upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency", where such notice is for "unlawful acts relatable to Article 19(2)".
- The portion under Rule 3(4) requiring intermediaries to take down content based on user notice has been struck down. However, this does not mean that users cannot send notices or that intermediaries should not act on it. It instead means that no liability attaches to intermediaries who fail to act on user notices.
- Failure by intermediaries to act on a government notice or court order would lead to the removal of the protective cloak of Section 79. In such cases, intermediaries could be subjected to prosecutions, as accessories or abettors to a crime.

The recent announcement by the Ministry of Electronics & Information Technology (MeiTy) of a possible civil remedy for expedited takedowns may provide succour to victims seeking expedited takedowns.[59]

d. *Prajwala* Effect on Intermediary Liability

In *Prajwala v. UOI,* the Supreme Court evaluated the use of Artificial-Intelligence-enabled tools to identify and quarantine content that may be identified as child sexual abuse material (CSAM) and

[58] *Ibid*. 54.

[59] https://www.hindustantimes.com/india-news/social-media-moderation-government-plans-new-platform-to-flag-online-posts-101613680077473.html

rape and gang rape videos (RGR) before they are uploaded or circulated online, and allowed for unblocking such content only after human verification affirms it to not be CSAM or RGR. Pursuant to consensus proposals put forth by the government committee formulated by the Supreme Court in this matter, several remedies were implemented through the apex court's order dated October 23, 2017.[60] The solutions evolved through the consensus process included setting up of the online portal www.cybercrime.gov.in to enable online filing of complaints of cyber crimes, inclusion of warning ads by search engines upon searches for CSAM or RGR, blocking of future uploads of identified content, and removal of identified content from other sources.

In addition, changes to reporting mechanisms on content hosting platforms and chat apps were implemented pursuant to the orders in *Prajwala*.[61] Issues such as the absence of specific buttons for reporting abuse, or obscure placement of reporting options were rectified to ensure easy and uncomplicated reporting mechanisms. Remedies for victims today, therefore, exist not only through law and regulations but also through these self-regulatory mechanisms of social media platforms.

One of the most significant proposals, which is part of the above Supreme Court order, is for content hosting platforms to research AI-enabled tools that can identify CSAM/RGR content. These remedial measures evolved for specific forms of gendered violence online are promising tools to combat online sexist hate speech and cyber VAWG.

> Women stated that online platforms do not provide adequate remedies, which, in turn, adversely affects the conduct of women online, including through self-censoring, limiting interactions, or sometimes even exiting the platform – all to avoid the toxic violence and abuse.

Since the above order in 2017, the use of AI-enabled tools to filter and moderate content online, especially those pertaining to hate speech and fake news, has increased significantly. However, the deployment of such tools for protecting victims of online misogyny and/or cyber VAWG remains pending.

Each content hosting platform is required under laws of multiple jurisdictions to put up notices that warn against uploading or circulation of unlawful content, and they do indeed carry these notices. Yet, Amnesty International's Toxic Twitter Report finds that women are forced to remain silent in the face of online violence owing to gaps in the policies and practices of intermediaries. Women

[60] (2018) 15 SCC 551.

[61] *Ibid*. 20.

interviewed by Amnesty as part of this report stated that online platforms do not provide adequate remedies, which, in turn, adversely affects the conduct of women online, including through self-censoring, limiting interactions, or sometimes even exiting the platform – all to avoid the toxic violence and abuse.[62] The protection of free speech, which formed the basis of the introduction of Section 230 of the CDA, appears to have fallen victim to the unfettered violence online and its chilling effect.

5. Regulating Intermediaries – A Global Overview

Several jurisdictions – with Australia leading the fray – have moved from a 'soft' self-regulation regime for intermediaries to stringent social media regulations, especially with respect to the sharing of violent, unlawful content.

Australia's Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act, 2019[63] provides for situations similar to the one the Indian Supreme Court dealt with in *Prajwala v. UOI.* This enactment criminalises sharing of "abhorrent violent material" and "abhorrent violent conduct" online. ("Abhorrent violent conduct" includes terrorist acts, murder/attempt to murder, torture, rape, and kidnapping.) Whilst this enactment mandates takedowns and not pre-filtration, it does reduce the timeframe for such takedowns.[64]

Germany has the *Netzwerkdurchsetzungsgesetz* or Network Enforcement Act to combat fake news, hate speech, and unlawful content. Malaysia's Communications and Multimedia Act 1998 regulates online content through the Malaysian Communication and Multimedia Commission set up under the Act. At the moment, there is little to no harmonisation across jurisdictions to have a unified stance against online violence against women.

The United Nation's Sustainable Development Goals (SDG) 2030 call for gender equality, peace, security, and strong justice institutions. These may only be achieved through a concerted effort of cross-jurisdictional collaboration. In the G7 meet of 2019, the Charter for a Free Open and Safe Internet[65] was proposed. Most G7 countries and some non-G7 countries such as Australia and India

---

[62] Amnesty International (2018), Toxic Twitter, a toxic place for women, available at https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

[63] Effective as of April 6, 2019.

[64] Refer: Nappinai N. S. (2020). "Rethinking Social Media – Through the Prism of Freedoms, Liberties & Victim Rights", (2020) – Published in the Festschrift Book for Nani Palkivala titled "Essays & Reminiscences" by LexisNexis for a more detailed discussion on victim centric social media legislations.

[65] Charter For A Free, Open And Safe Internet, Aug 21, 2019, DGE. https://www.entreprises.gouv.fr/files/files/directions_services/numerique/Charter-for-a-free-open-and-safe-Internet.pdf

signed the Charter, as did some social media platforms. However, with the US backing out at the last moment, this effort to ensure safer online spaces was thwarted. The significance of this Charter is in the goals listed, which echo the proposals put forth in *Prajwala v. UOI* for social media platforms to act responsibly, and filter violent, illegal content. With uncertain safety online, the freedom for women and girls and gender equality in cyber spaces will remain an empty right with vacuous remedies.

Most social media platforms fall under US jurisdiction, and enjoy the safe harbour protection of Section 230 of the CDA. This has meant an uphill battle for law enforcement agencies attempting to institute takedowns. However, the US has started tightening its stand on regulating cyberspace with its recent move to combat CSAM, removing exemptions for companies that fail to police illegal content.[66]

Any democracy ought to – and strictly so – protect its crucial right to free speech and expression. However, this cannot erase victims' rights. The rights to dignity, privacy, and protection against violence and hatred are all as inherent to human rights as free speech. Nation states will have to provide due protection to free speech without compromising the rights of the victims of cyber VAWG. This would entail maintaining the fine balance between reasonable restrictions and legislative mandates for compliance without overreach or prohibitive restrictions that can chill free speech.[67]

6. Future of Law to Combat Misogyny as Hate Speech

a. Inclusion of Gender in Hate Crime Laws

Presently, laws across multiple jurisdictions, including the UK,[68] Singapore,[69] Japan,[70] and the EU, do not include gender under the ambit of hate crime laws. Policy discussions regarding this remain conflicted. There is uncertainty on whether including gender as a category under hate crime laws would hamper or help prosecutions and the consequent deterrence of gendered hate crimes.

---

[66] https://www.nytimes.com/2020/03/05/us/child-sexual-abuse-legislation.html

[67] *Ibid*. 64.

[68] Public Order Act, 1986.

[69] Singapore Penal Code http://www.vertic.org/media/National%20Legislation/Singapore/SG_Penal_Code.pdf

[70] Japan Hate Speech Act https://www.hurights.or.jp/archives/focus/section3/2016/09/japans-hate-speech-elimination-law.html

Meanwhile in India, pursuant to the Supreme Court's decision in *Pravasi Bhalai Sangathan v. UOI*,[71] the Law Commission researched hate speech, and in its Report on Hate Speech (2017),[72] recommended the inclusion of gender as a category of hate crime under the IPC.

Hate crimes are dealt with under Section 153A of the IPC ("Promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony") and Section 153B of the IPC, which deals with hate speech through imputations and assertions prejudicial to national integration against members of any "religious, racial, language or regional group or caste or community".

The proposed provision set out by the Law Commission in its report, and extracted below, is yet to be added to the statute:

153C. Whoever on grounds of religion, race, caste or community, sex, gender, identity, sexual orientation, place of birth, residence, language, disability or tribe - (a) uses gravely threatening words either spoken or written, signs, visible representations within the hearing or sight of a person with the intention to cause, fear or alarm; or (b) advocates hatred by words either spoken or written, signs, visible representations, that causes incitement to violence shall be punishable with imprisonment of either description for a term which may extend to two years, and fine up to Rs 5000, or with both.

b. Expanding Existing Provisions/Crafting New Laws

Existing provisions, if enforced effectively, could also alleviate the travails of cyber VAWG, as was demonstrated by the Delhi High Court in its decision in *Swami Ramdev v. Facebook Inc & Ors*,[73] wherein the defendants were directed to "take down, remove, block, restrict/disable access, on a global basis", and not just limit blocking to a particular geographic location.

India is also contemplating reviewing its criminal and cyber laws, including the IT Act. It is on the cusp of evaluating amendments to its Intermediary Rules, the drafts for which were circulated for public response in 2018. Whilst undertaking this review, it is important to centre victims' rights and empower them to support prosecutions through active participation and/or to seek accountability from the justice system. Similarly, it is important to keep in mind that victims are reluctant to approach law enforcement or courts, and to compel them to do so for all forms of takedowns dilutes their rights to effective remedies. Hence, while reviewing the Intermediary Rules, it may be

[71] AIR 2014 SC 1591.

[72] Law Commission of India, Hate Speech, (Report No. 267, March 2017). Available at: http://lawcommissionofindia.nic.in/reports/Report267.pdf

[73] 2019 SCC OnLine Del 10701: (2019) 263 DLT 689.

expedient to provide a mechanism to ensure the takedown of illegal content through user notices and upon actual knowledge, as was envisaged under Section 79 of the IT Act, while keeping in mind the findings in *Shreya Singhal.* MeiTy's actual proposal for expedited takedowns is not still in public domain and its efficacy therefore remains to be evaluated. Removing ambiguity and ensuring checks and balances may be one lesson that could be adopted whilst deciding on inclusions to existing legal frameworks.

At this juncture, India has multiple options, including continuing the present structure of covering cyber crime provisions under multiple legislations, or bringing them all under one new, standalone legislation. An evaluation and crystallisation of its position on intermediary liabilities is an integral part of the way forward.

c. Recommendations

It would be pertinent for lawmakers to evaluate enforcing laws to counter online violence against women, either under general criminal laws, hate crimes, or both. While doing so, there needs to be sufficient clarity in the restraints on speech that the law mandates, and the modalities for its implementation.

Formulating such legislation requires a focus on the Indian ecosystem, its socio-legal, socio-economic, and cultural diversity. Mindless adaptation of laws from other contexts will only result in repeating a two-decade old problem with respect to the IT Act of 2000.[74] While the discussions here pertain to the specific threat of online hate speech and hate crimes, the proposed legislation should address a wider spectrum of threats. In doing so, it should evolve a forward-thinking legislation that takes note of emerging technologies and their vulnerabilities, provides protections against national, economic, and individual threats, and withstands judicial scrutiny on constitutionality and the test of time.

A wishlist for effective laws to combat online crimes against women should include:

- Precise and clear provisions that specifically address offences against women.
- Provisions that can be easily understood by an ordinary person, thus acting as a deterrent.
- Laws and regulations focusing on victims' rights. This would include a review of constructs that treat offences under substantive criminal provisions as State Prosecutions, treating

[74] Interpretation of Sections 65A and 65B of the Indian Evidence Act, 1872, which were borrowed from a UK provision, which in itself was repealed before India's 2000 amendment to the Evidence Act, is still being debated and decided upon with little clarity. Refer: Electronic Evidence – The Great Indian Quagmire: (2019) 3 SCC J-41; Compliance With Sections 65A & 65B Indian Evidence Act, 1872 – A Practical Guide for Practitioners (https://www.cybersaathi.org/elementor-7514/); and From Anvar to Arjun – A Tale of Two 'Anys' (https://www.livelaw.in/columns/from-anvar-to-arjun-a-tale-of-two-anys-other-stories-157264).

victims as mere witnesses to the crime, and effectively keeping victims out of the remedial process.

- Simple and easily adaptable procedures for filing complaints and tracking them. For this, both the IPC and the Criminal Procedure Code, 1973 should be reviewed.

Further, while awareness plays a significant role in mitigating crimes, it would be most effective if the focus is on restraining criminals instead of advocating safe conduct rules for victims. Enforcement agencies ought to note that their message for prevention or protection would only be as effective as their actual implementation of the letter and spirit of the law. As Bleich[75] warns, when laws are not backed by any prosecutions or convictions, they become "symbolic", "lose their effectiveness", and become "empty rhetoric".

Finally, India should review its position, and either consider ratifying existing conventions or spearhead a movement towards evolving a cohesive and universally adaptable alternative to an international instrument for cross-jurisdictional collaboration. Either way, it is clear that India needs methodologies for international enforcement of cyber crimes. This need must be met expeditiously. We are inexorably moving towards a "Digital India", and the threats and vulnerabilities that this domain poses are bound to increase exponentially. At this juncture, India cannot afford to resort to reactive measures in law or policymaking as it is wont to, but has to proactively address this need, considering not just existing but evolving threats. In doing so, the imperative to address technology mediated crimes against women cannot be ignored.

> If online misogyny is to be dealt with, the addition of laws or regulations, however stringent they may be, is insufficient. These laws must also be strongly enforced.

If online misogyny is to be dealt with, the addition of laws or regulations, however stringent they may be, is insufficient. These laws must be strongly enforced, failing which the "broken windows of cyberspace"[76] would merely embolden criminals to intensify their attacks. Deep-rooted prejudices, assumptions of immunity from action, and absence of the fear of retribution are just some causes that hamper any attempt at combating online VAWG. Justice delivery systems ought to be revamped to visibly demonstrate their effectiveness so they can act as deterrents.

---

[75] Bleich, Erik. 2011. "The Rise of Hate Speech and Hate Crime Laws in Liberal Democracies." Journal of Ethnic and Migration Studies 37(6):917–934.

[76] Nappinai N. S. (2017). Technology Laws Decoded. LexisNexis.

The path for reining in cyber VAWG remains open, both internationally and for India. With the Additional Protocol to the Convention on Cybercrime on the anvil, moves towards listing technology-mediated crimes against women as sexist hate crimes are imminent. For India, the present initiative to review its various laws is an opportunity to ensure that well-defined laws – harmonised internally and with foreign laws – are formulated to secure effective enforcement. Finally, while drafting statutes, the words of the Delhi High Court in *Swami Ramdev v. Facebook Inc*[77] ought to be kept in mind; that for any Statute to be respected in its "letter and spirit", orders of the courts, pursuant to such laws, need to be implemented fully and effectively. If a law lacks teeth, it would remain mere rhetoric and fail in its purpose of protecting and remedying victims.

---

[77] *Ibid.* 73.