Evolving robust responses to gender-based cyber violence

New strategic directions

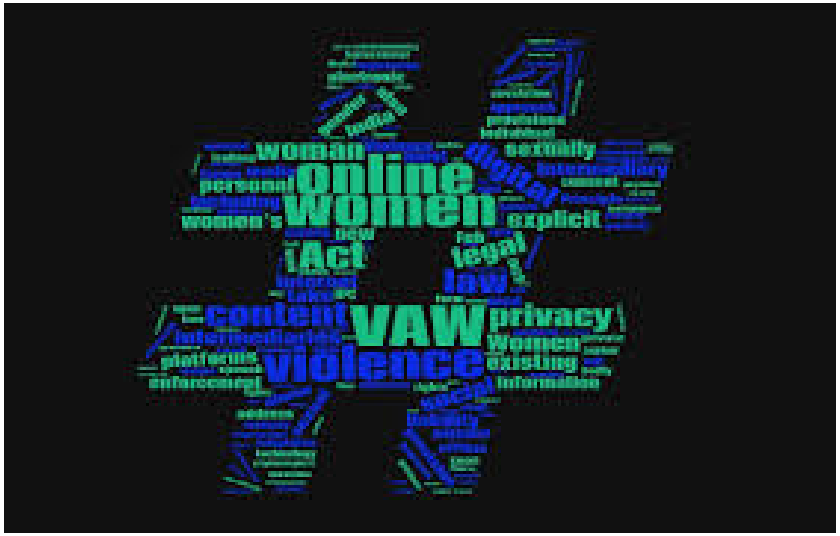
Anita Gurumurthy
IT for Change

COPPS, May 2018

1. Gender-based cyber violence: an overview

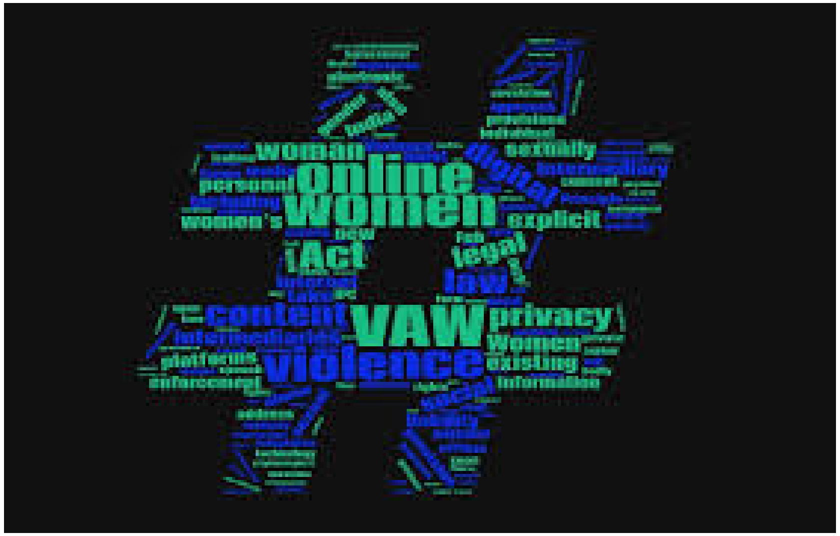
1.1 Defining gender-based cyber violence

- Acts of gender-based violence that are committed, abetted or aggravated, **in part or fully,** by the use of Information and Communication Technologies (ICTs).
- The online communication environment – Invisibility, anonymity and asynchronicity leading to toxic disinhibition
  - Harassment on web and mobile platforms, sexual or not - cyber-bullying and trolling
  - Doxxing
  - Creating fake profiles of women with an intent to defame/harass them
  - Non-consensual circulation and malicious distribution of private material, including intimate pictures and sexually explicit material.

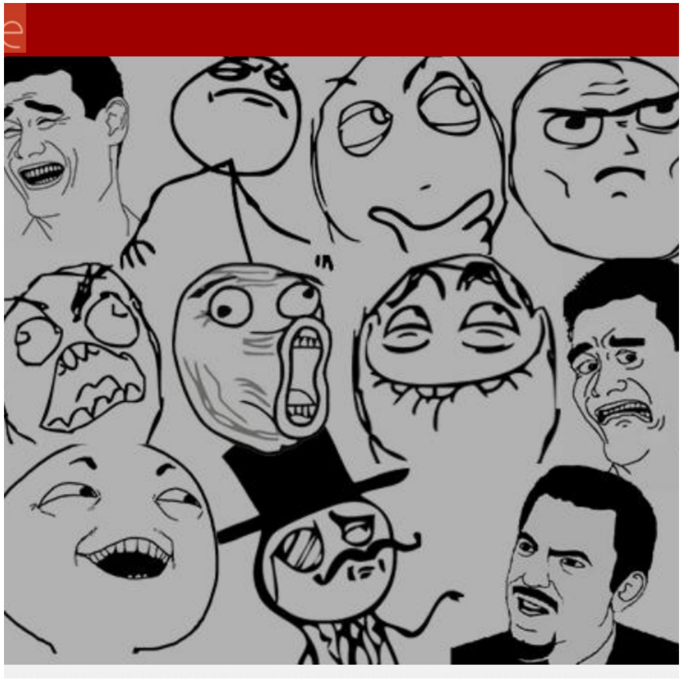


1.1 Defining gender-based cyber violence

- There is a continuum between offline violence and violence in and through digital spaces.
  - Stalking
  - Impersonation that ends up in violence
  - Circulation of rape videos

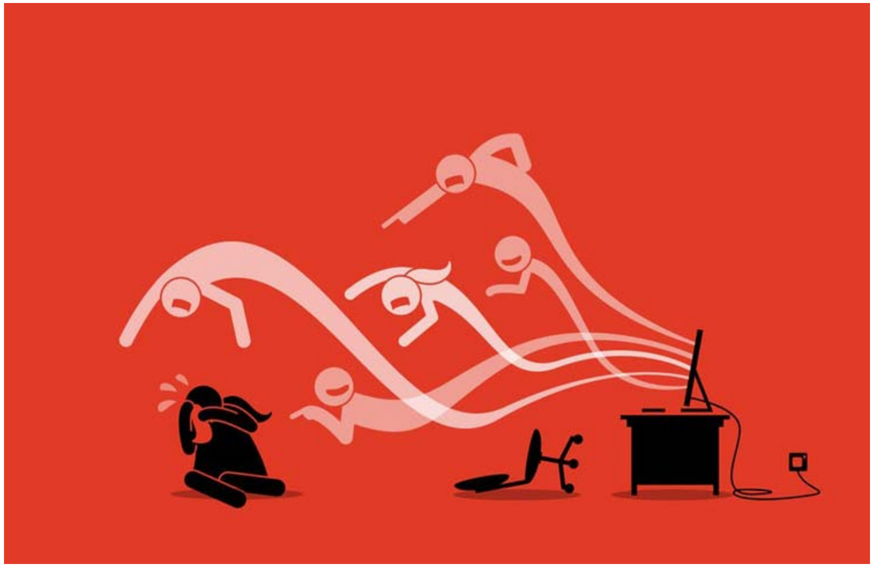


1.2 Pervasive problem



- Cuts across all socio-structural locations
- Reflects deep social bias
- A tool to silence women, especially those active in public-political spaces
- Ubiquity – non-consensual circulation of content, perpetrator too close for comfort?
- Phenomenon itself morphing with technology diffusion – poses difficulties for law enforcement
- Reluctance of victims to take recourse to law

1.3 What we are responding to is the tip of the iceberg



Feminism in India – online survey

36% respondents took no action

28% reported that they had intentionally reduced their online presence after suffering online abuse.

30% respondents said they were not aware of laws to protect them from online harassment.

Only a third of respondents had reported harassment to law enforcement; among them, 38 percent characterized the response as “not at all helpful.

2. Key gaps/challenges in legal-institutional responses to gender-based cyber violence

2.1 Gaps in existing laws

- Pre-digital legal frameworks unable to make the shift that required to deal with the ‘digital’ phenomenon. (Fundamental concepts of “jurisdiction” and “culpability” need to be re-interpreted)
  - *Each time that a non-consensual image of a woman is shared, there is a fresh act that infringes upon her right.*
- Sexist speech that is not sexually explicit is not addressed through existing laws on hate speech – so there are no clear provisions under which generalised, misogynystic trolling can be booked.
  - T. K. Viswanathan expert committee set up in 2017
  - Recommendation for recognition of gender identity and sexual orientation as legitimate grounds for hate speech.
  - However, wording vague, refers to ‘incitement of offense’, a much lower threshold for hate speech compare to ‘incitement of violence’.

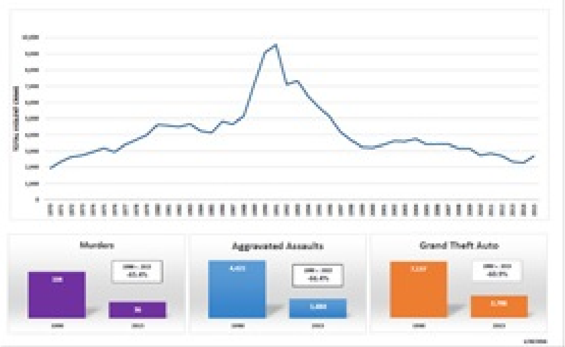
2.1 Gaps in existing laws

- Privacy-and-consent approach adopted in piecemeal ways – without an understanding of bodily privacy as much more than images of intimate parts.
  - Research reveals that officials are much more likely to use obscenity-based provisions of the IT Act (Section 67A, Section 67B) rather than the privacy and consent provisions (Section 66E) when booking cases of violence.
  - Section 66 E has a narrow framing of privacy which limits the idea of bodily privacy to images of private parts.

2.2 Shortcomings of law enforcement responses

- Police officials’ own biases and prejudices (“only bodily violence is real”, “distinction between good victim and bad victim”).
- Police officials are constrained by the shortcomings of existing legal framings. Pace of change needs ongoing capacity building (eg. Exploring creative ways to read Section 66E – revenge porn)
- Difficulties in obtaining cooperation of Internet intermediaries for digital evidence gathering (Bengaluru – morphed picture case)

2.2 Shortcomings of law enforcement responses



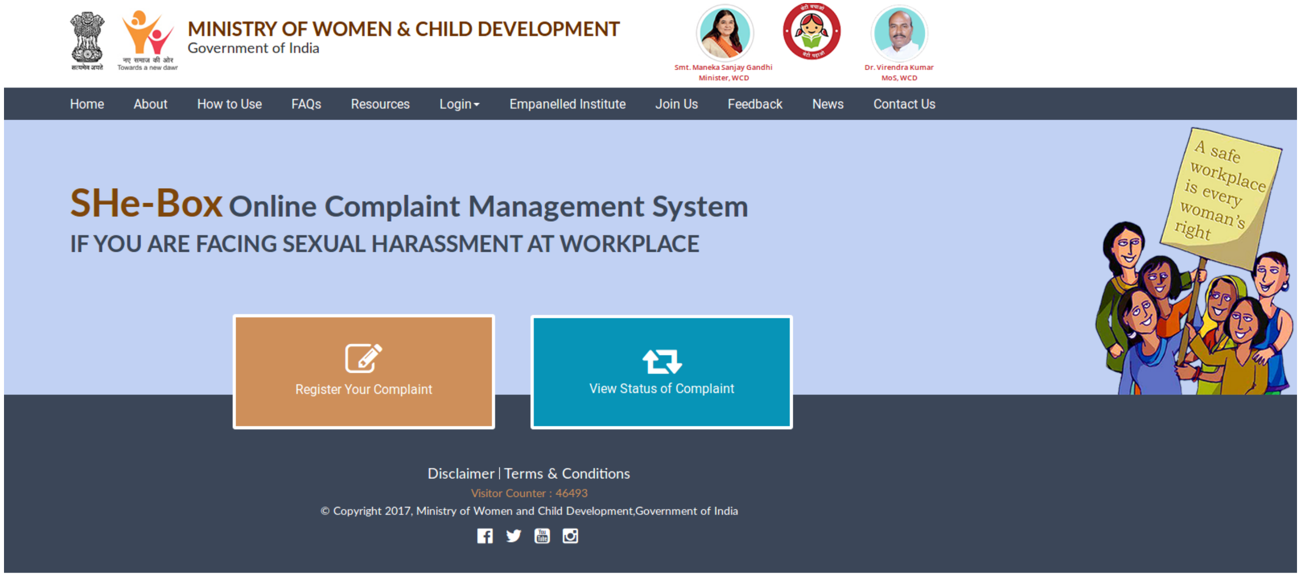
- Gaps in existing statistical systems (NCRB data systems)
  - Record only of ‘principal offense’ - in rape cases where the rape is videotaped and circulated on the Internet, such instances put down as rape in the statistical system
  - **Chapter on Cybercrimes** - only reference to violence against women is a table that ranks different types of cybercrimes according to motives.
  - ‘Insult to the modesty of women’ is the only one presenting a gender disaggregated picture. (what are the sections included here other than sections 67 and 67 A of the Information Technology Act (2000))
  - Fails to cover certain crimes booked under provisions of the Indian Penal Code - Section 354C (voyeurism) and Section 354D (cyberstalking)
  - **Chapter on Crimes against Women**, the only reference to cyber crimes is to cases that have been booked under Section 67 A of India’s Information Technology Act (IT Act) – publishing or transmitting of sexually explicit material. Other forms of technology-mediated violence are not captured at all.
- Failure to use Police Modernisation Fund effectively for building forensic lab infrastructure and developing training capacities (CAG 2016)

2.3 Lack of holistic institutional responses

- **One stop crisis centres** that seeks to integrate medical aid, psycho-social counselling and police services proposed under the Nirbhaya Fund have not taken off. Of the 458 crore allotted to this fund in the past 3 years, only 81 crores were utilised between 2015-18.
- For Women's Helplines, also proposed under the Nirbhaya Fund, out of the 156 crore allocated, only 21 crore has been disbursed.
  - A 2017 Human Rights Watch research study reveals the inefficacy of the One Stop Centres (OSC) that are intended to backstop the national helpline on GBV :

    ".....the OSC scheme was set up hastily, without meaningful consultations with local rights groups and NGOs already running crisis-intervention centers in different parts of the country operating in hospitals, police stations, or courts. The government also failed to integrate these existing centers or build on good practices from models developed in various parts of the country. It did not maximize its reach to victims of gender-based violence who usually come to hospitals, police stations, and courts." (Human Rights Watch, 2017).

2.3 Lack of holistic institutional responses



MINISTRY OF WOMEN & CHILD DEVELOPMENT
Government of India

Smt. Maneka Sanjay Gandhi
Minister, WCD

Dr. Virendra Kumar
MoS, WCD

SHe-Box Online Complaint Management System
IF YOU ARE FACING SEXUAL HARASSMENT AT WORKPLACE

Disclaimer | Terms & Conditions
Visitor Counter : 46493
© Copyright 2017, Ministry of Women and Child Development,Government of India

- New cyberviolence initiatives of Ministry of WCD – centralised and disembedded from local systems (She-Box)
  - Ministry does not play any role except channeling the complaint to existing resolution mechanisms
  - The majority of workplaces have not constituted an Internal Complaints Committee, despite it being mandatory under the law
  - Similarly, in most state governments, “functional local complaint committees are lacking”

3. Strategic directions

3.1 The law

- A single comprehensive legislation on gender-based cyber violence going beyond piecemeal tinkering of the IPC and the IT Act.
- Gender-based hate speech provision rooted in an anti-discrimination framework
- Nuanced debate on online content regulation needed – using the opportunity before us in the form of the constitution of the Content Regulation Committee. (MWCDs guidelines abt responding to online trolling)
- POCSO and cyber violence -- we need effective guidelines that recognise online grooming as an offence
- DV Act - Definition of mental/emotional abuse -- expand this to include intimate partner violence in online spaces.

3.2 Law enforcement

- Capacity-building of police officials to provide support to victims and to creatively interpret existing legal provisions to book perpetrators of cybercrime.
- Digital forensics and digital evidence processing – specific protocols need to be put in place.
- NCRB – stats should reflect the full picture of the phenomenon of genderbased cyber violence. Aggregate stats on cyber violence should be proactively disclosed at the state level.
- How can we hold Internet Intermediaries accountable – is harmonization technical?
- DV Protection officer and protection order -- measures needed to issue restraining order against intimate partner violence in online spaces.

3.3 Institutional responses

- Partnerships – workplace, crisis centres, educational institutions, local communities
  - Moving beyond textbook responses of CCTV camera and Safe City projects – a different approach is needed to
  - Interpreting the Women’s Security agenda in the 25,060 crores in the Police Modernisation Ffund approved by the Cabinet
  - Nirbhaya scheme – strengthen implementation of one-stop-shop centres and women’s helplines and introduce local audits.
  - Holistic strategy on cyberviolence that is decentralised and focuses on involvement of local agencies in implementation
  - A new sub-track on women’s online security in the Women’s Security domain of the Police Modernisation Fund.
  - Safe cities – use of GIS for tracking unsafe spaces; move beyond the CCTV paradigm.

3.4 Institutional responses – educational institutions

- The University Grants Commission (UGC) guidelines that prescribe Internal Complaint Committees to appoint a student representative.
- Unless a complaint is made to the ICC - that is, consent is given by the woman – due process cannot begin.
- While the UGC has also said that the ICC has to take complaints made by individuals from gender discriminated locations, it has not laid down any guidelines in this regard.
- While the mandate of the ICC is prescribed by the law, to ensure full justice, it may have to go above and beyond such mandate.

Thank you

anita@ITforChange.net