Born digital, Born free?
A socio-legal study on young women's experiences of online violence in South India

IT for Change | 2019

Executive Summary

Introduction

Digital technologies have generated unprecedented ways of being and doing, dramatically changing the social and economic order. Recoding human subjectivity and social interactions, they recast power relationships. Gender relations are centrally implicated in this shift to a networked sociality where the online and offline must be understood as non-dichotomous. This research study examined how the born-digital generation of young female adults – who live their lives in the criss-crossing of the real-digital – grapple with the challenges of navigating digital space in the face of cyberviolence. Through a survivor-centred, feminist approach, it sought to unpack the fluidity between human subjectivity, social ideologies, legal norms, institutional rules and digital networks.

World over, young women are disproportionately affected by cyberviolence. Through a quantitative survey with 881 women aged 19-23 years and qualitative explorations with their male peers and other key stakeholders, this study looked at how young women experience cyberviolence. The research sites included metropolitan cities and small towns in the southern Indian states of Karnataka, Kerala and Tamil Nadu.

Key findings

1. Cyberviolence is pervasive

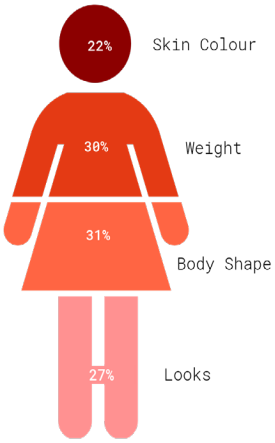
Over one-third of survey respondents have faced harassment, abuse or unwanted behaviour online and two-fifth are aware of other women in their circles who have had similar experiences. A quarter of the respondents who had faced cyberviolence reported that the identity of their perpetrators was known to them, whereas half reported that the perpetrator was unknown. Some had experienced harassment from both known and unknown perpetrators. Also, 90% of respondents who had faced harassment reported that they had been harassed on multiple occasions.

2. Over three-fourth of respondents have faced gendertrolling

Bullying based on physical attributes emerges as a common form of violation experienced by young women. 31% of respondents who have faced cyberviolence reported being bullied about their body shape; 30%, their weight; 27%, their looks; and 22%, their skin colour.

Irrespective of social location, women face demeaning commentary about their physical bodily attributes. Research on body shaming points to how, given the affordances online platforms offer for projecting and comparing one's appearance, women begin to engage in self-surveillance, trying to meet tacit standards of desirability.

Women online are bullied based on a range of physical characteristics



Women from marginal social locations face particularly heinous forms of gendertrolling that denigrate their social identity. Misogynistic vitriol faced by dalit women is also casteist.

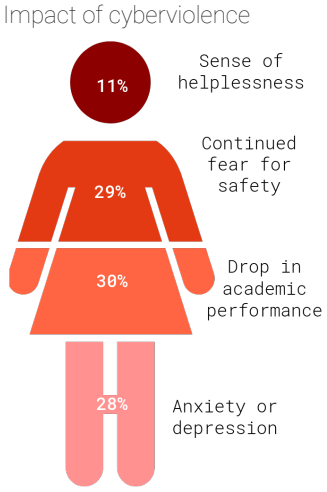
3. Over 80% have faced online sexual harassment of some form

The most commonly reported forms of sexual harassment were cyberstalking/being contacted repeatedly by the same person demanding a sexual relationship (44%), followed by doxxing/ instances of personal information being leaked online or fake profiles being created (39%) and sexually explicit images/photos being shared with an individual without her consent (30%).

Not all acts of stalking are perpetrated by strangers. Oftentimes, stalkers are likely to have been former partners/friends/ acquaintances with whom the victim has cut ties. In the case of doxxing, many times, there is also a threat to release a woman's photo morphed with another pornographic image. Women also reported receiving unsolicited 'dick pics', a type of harassment noted to be so widespread that women have started groups on Snapchat, Instagram etc., to deal with the problem. Women in public life are seen as easy game, to be pushed back and punished with malicious and sexualized attacks. Male power and privilege manifest online through a routinization of such sexualized assertions over women.

4. Consequences of cyberviolence are very real – ranging from physical, psychological to social, functional and aspirational impacts

Nearly one-third of respondents who faced cyberviolence reported that the incident had affected their academic performance at some point. Victims also experienced disruptions to their everyday functioning and routines. In fact, 6% reported to have attempted some form of self-harm.



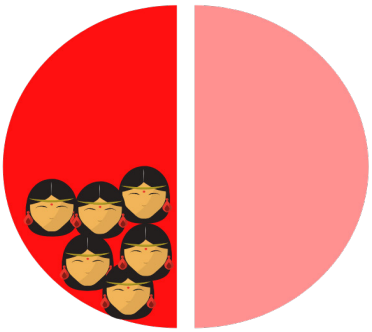
29% of the 326 respondents who faced cyberviolence reported that they continue to feel scared for their safety; 28% felt anxious or depressed; and 11% reported being besieged by a sense of helplessness.

Violence has a chilling effect. After being attacked, nearly 40% of respondents who had faced cyberviolence reported having reduced use of their mobile phone and laptop and deleting their social media accounts. Similarly, upon hearing about harassment faced by women in their circle of friends and acquaintances, over 57% answered that they have become cautious of posting content on their social media.

5. Rather than come out and seek support, women may simply adjust to cultures of cyberviolence, in order to preserve their space of agency

Quitting the web altogether is not realistic and may entail huge social, economic and personal costs for women. Consequently, women adjust to unrewarding and penalizing aspects of their digital lives, fashioning their presence and participation to preclude the possibility of censure or violence.

More than half of those who faced cyberviolence did not seek parental support



Many of them were worried their gadget may be confiscated

54% of respondents who had faced cyberviolence reported that they did not seek help from parents or relatives. Nearly half of this number reported that this was because they were worried their mobile phone/ laptop/gadget may be confiscated.

6. Gender hierarchies don't go away in digital sociality; they get reconfigured

Numerous instances of household-level monitoring and surveillance of young women's use of digital technologies were reported in the qualitative inquiry. In Tamil Nadu, some young women reported that they were not allowed to have their own smartphones and had to use their brother's phone when they went online. In Kerala, the research found instances of young women having to share their passwords with male family members.

Social surveillance also manifests in grouptrolling. While cybermobs may be uncoordinated attacks by multiple men across places, quite paradoxically, a digitally networked environment also encompasses inscrutable, hyper-local fraternities for the conduct of manhood; all-male 'bro-clubs'.

Young male students in Kerala told researchers about local young men's WhatsApp groups named after particular places – Kattancherry boys, Kaverinagar boys etc. (names changed). In these homosocial private male spaces, men build a new-age machismo, getting fluent with expletives, making sexualized memes to assert male entitlement, 'hooking' women or chatting them up using fake profiles, and watching porn.

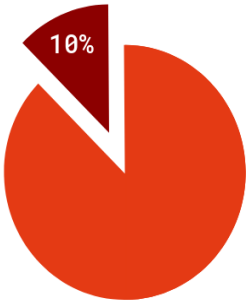
-Male participant,FGD, Tamil Nadu

But, somehow, women navigate the surveillance minefield, carefully negotiating risks and rewards. They may just laugh it off, or become digital Cinderellas who surreptitiously manage dual identities of the 'good' and 'bad' girl, or caution each other to steer clear of trouble.

7. Survivor-centred institutional response mechanisms are missing

Although mandated by the law, internal committees on sexual harassment in colleges are mostly non-existent or where present, dysfunctional and ill-prepared. Hostile college authorities intimidate students, preventing them from bringing up complaints, whilst students who do step up may easily be victim-blamed.

Despite facing cyberviolence, very few women approached the police



Of the 326 respondents who had faced gender-based cyberviolence, only 13% approached college authorities.

Law enforcement agencies tend to adopt a protectionist approach at best and a victim-blaming judgementalism at worst. Fear of police insensitivity was a significant reason for not seeking their help.

Of the 326 respondents who faced cyberviolence, a mere 10% sought assistance from the police.

Given limitations of resources and the tedious pursuit of digital

evidence, the police tend to de-prioritize cases of gender-based cyberviolence, trading off investigations in cyberviolence for 'more serious' cybercrimes, like cyberterrorism.

8. There are major gaps in existing legal frameworks with respect to addressing gender-based cyberviolence

> Now you have to look; is there a sexual aspect? Is there obscenity? If so, evoke the relevant sections; if not, apologize and tell [the victim], the chances of justice are slim.
>
> **- Police official, key informant, Kerala**

The repeal of Section 66A of the IT Act leaves women with very little recourse to pursue cases of gendertrolling. Misogynistic speech is not recognized as grounds for hate, and the police and lawyers find it difficult within other sections of the Indian Penal Code (IPC) to establish a case that stands in court. To deal with online sexual harassment, the police prefer to deploy anti-obscenity sections rather than provisions rooted in privacy and consent. They are also not updated with the latest judicial decisions. This leaves much to be desired for the feminist pursuit of justice.

9. Marshalling digital evidence is fraught with innumerable hurdles

Producing admissible digital evidence in court is complicated not only by poor compliance to Standard Operating Procedures by investigating officers, but also by varying interpretations in Courts of certification standards. Obtaining the cooperation of foreign internet intermediaries implicated in evidence-gathering poses jurisdictional challenges often impossible to overcome.

> It takes a long time; police request for evidence, Facebook (FB) takes 20 days, then FB asks for more information, police responds and again, FB takes 20 days to respond. This negatively impacts the investigation process. There are also lots of technical issues. We end up moving from desk to desk in the FB offices in order to get permissions.
>
> **- Police official, Key informant, Karnataka**

Conclusions

What the study concludes is that even as digital space opens up an exciting new frontier for young women's self-building, intimacy, public expression and more, the techno-architectures of the platform economy are not necessarily liberating. Norms and practices of digital space do not seem to erase gendered hierarchies. On the contrary, even though they are contested by feminist actors and actions, oppressive gender relations continue to prevail in the contemporary configurations of society.

1. Capitalist digital architectures generate regressive social arrangements that perpetuate retrograde gender norms and practices

Under surveillance capitalism, platform design prioritizes virality, feeding content to maximize clicks. Image-based cultures of social media platforms – characterized by selfies and evaluative photo commentary – reward and reinforce gender performance based on accepted gender norms and roles. Young women project femininity and respectability, and men, masculinity and aggressiveness. Women who transgress are penalized through mob-trolling. Such violent gender cultures negatively impact the civil-political rights of women and their aspirations to be part of the public sphere. Not only are women denied their full citizenship, but such marginalization is inimical to democratic discourse itself.

2. Gaps in the law perpetuate the naturalization of gender-based cyberviolence, reinforcing a culture of silence that prevents women from seeking redress

The trivialization of cyberviolence – by harassers, by law enforcement agencies, and many a time, by victims themselves – is in part because the law is unable to capture and record the mutations of gender-based violence emerging in digital sociality. By ignoring the harms caused by online violence, the legal system itself becomes complicit in their trivialization.

The result is that the meta narrative of what is justice is itself unjustly framed, thus depriving women of the very right to make a claim. The continued use of oppressive, anti-obscenity sections is part of the systemic misframing of gender justice. Research suggests that where there are laws against cyberbullying, it has an encouraging effect on women's online participation. Legal reform is therefore an important instrument to tackle gender-based cyberviolence.

3. Though platform intermediaries have introduced new features for enhanced safety, their response to gender-based cyberviolence typically hides behind the smokescreen of difficult-to-fashion 'community standards' or a blatant transfer of duty to the state

The take-down of offending content becomes an urgent priority for women who face cyberviolence. To address this concern, dominant social media companies have, over time, introduced new design features for improved user safety and security. This is an individual, even if important, fix, and far from adequate as a systemic response. Platforms do not seem to have a solution to the quandary of contextually interpreting women's human rights standards in different cultural contexts. In India, they have taken the view that the business of securing women's rights is the sole responsibility of the state. They have argued that their liability extends only to compliance with official rules, and that the state must set up the requisite institutional mechanisms to identify and flag illegal content.

Automated filtering of patently illegal content and the traceability of its origin for law enforcement purposes does remain a vexatious issue. However, as gatekeepers of social and public interaction, platform companies need to step up to reexamine their role towards a healthy public sphere. As things stand today, the remote possibility of any redress for women who approach such platforms gets invariably caught up in the rhetoric of 'community standards' that platform companies use to justify opaque actions that are accountable to no one.

4. Survivors invariably do not step up to seek help given the high moral panic associated with young women's sexuality and deep-rooted institutional patriarchies

The stigma and moral panic associated with women's sexual expression and victim-blaming extends across all social institutions – from the household to the police and educational institutions. This means survivors who wish to seek institutional redress must be prepared to face patriarchal actors who will sit in judgment of their 'character', a cost that may be simply too high to bear.

The choice then is to take recourse to individualized solutions like blocking, flagging or reporting the perpetrator on the platform. This may work only in some cases, and the possibility that the perpetrator may create alternate profiles to continue the harassment is ever-present.

The current context seems to isolate victim-survivors, leaving them bereft of real options to seek psycho-social support and redress.

Recommendations

Gender-based cyberviolence is ubiquitous. A systemic change that calls for a rethink about the digital protocols of the communicative arena as well as the socio-cultural fabric of digitally mediated institutional relations is needed. Digital rights of women tend to be reduced in policy priorities to 'bridging the access gap', a foundational priority no doubt, but conceptualized as an end in itself. Digital strategies and gender strategies need to be integrated in a multi-layered way to enable women's digital citizenship. This means laying down both the pathways for digital enskillment, fluency and empowerment and the priority actions to ensure women's right to freedom from harm.

Existing efforts such as the cybercrimes portal do provide an important avenue for victims to reach out to authorities. However, digital strategies must be guided by a rights-based approach that informs, educates and guides. To address local patriarchal cultures, interventions also need to be situated in schools and other community settings. The underutilization of the Nirbhaya Fund is a sad reflection of the absence of a cohesive vision and coordinated execution towards gender-transformative social change. Outlays for the Fund need to be expanded to enable a well-coordinated programme based on inter-ministerial cooperation and built on district level efforts, that not only uses digital technologies as an 'innovative solution', but also recognizes the emerging social context in which digital technologies reshape gender relations.

Additionally, national and state level task forces with representatives from different government departments, law enforcement agencies and civil society actors – women's grassroots organizations, feminist scholars, educators, technologists, legal experts, mental health professions – need to be set up for strategy development, monitoring and review.

This section outlines below the priority actions that are required at the formal institutional levels: legal reform, survivor-centred institutional responses and platform governance.

1. Legal Reform 

A new law on sexual harassment, grounded in ideas of privacy, consent and women's dignity, is necessary to deal with emergent forms of sexual violence that are emerging in digital spaces such as doxxing, voyeurism, cyberstalking, involuntary pornography, and non-consensual circulation of intimate images. This will help overcome the current quandary where women victims have to resort to anti-obscenity provisions to deal with such situations.

Gender and sexual orientation should be included as protected categories in Section 153A and Section 505 of the IPC. Further, the law must shift its focus from 'incitement of violence' to 'harms to dignity', in order to effectively address the growing pandemic of gendertrolling.

The procedures for presentation and certification of digital evidence must be simplified. The more permissive reading of Section 65B of the Indian Evidence Act by the Supreme Court that allows for a waiver of the certification requirement of digital evidence in instances where a device is in adverse possession, must be applied in cases of cyberviolence. However, it is important that easing up of certification requirements does not promote illegal collection of digital evidence through invasive state surveillance.

In order to overcome the challenges in cross-border access to data due to the difficulties of enforcing extra-territorial jurisdiction under MLATs, mandating storage of data within India is one option, as recommended by the data localization provisions of the Srikrishna Committee Report. Of course,

indiscriminate state access to citizen data is not the goal, and any mandatory data localization should not be allowed to happen without effective privacy and personal data protection legislation.

Intermediary liability law and policy in India is in a phase of transition. A differentiated intermediary liability regime that takes into account differences in the user base, type and functionalities of platform intermediaries in defining responsibility and accountability for content must be put in place.

2. Survivor-centred institutional responses 

There needs to be a shift in the institutional cultures of formal redress mechanisms – the police, court systems and committees on sexual harassment in workplaces and colleges – so that patriarchal protectionism is replaced by survivor-centredness.

Police

Targets for training of police personnel under the Cyber Crime Prevention against Women and Children (CCPWC) scheme must be increased by all states. Specifically, more women police personnel must be trained under the scheme.

The personnel assigned to cyber cells or cybercrime police stations are very few and the ratio of crimes per investigating officer is highly skewed. Staff strength in cyber cells/cybercrime police stations, therefore, needs to be enhanced. There should be more women police officers posted at cybercrime police stations. The success of UP government's 'Women Power Line 1090' also demonstrates survivor-centred approaches that guarantee confidentiality and provide support to victims in remote filing of complaints.

Police should periodically carry out outreach programmes in colleges to raise awareness of the available legal and non-legal options in cases of gender-based cyber violence. Collaborative projects involving the police and women's rights organizations and counsellors need to be set up to provide psycho-social assistance to survivors, so that they can cope with the trauma of violence and navigate the stress of waging a legal battle.

Dedicated data on cybercrimes against women must be collected and reflected in the publication of crime statistics by the National Crime Records Bureau.

Courts

Judges and public prosecutors need to be trained for cultivating the knowledge, skills and attitude required to ensure gender equality in the digital context. This will go a long way in survivors' access to justice.

Judges must avoid taking a protectionist approach and be open to creative applications of the IT Act and IPC provisions that emphasize women's dignity, privacy and autonomy.

Free legal aid services are essential to ensure access to justice for survivors of violence who come from marginal socio-economic locations.

Internal Committees on Sexual Harassment

All colleges and higher education institutions must set up the Internal Committee (IC) on Sexual Harassment mandated by the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 and the University Grants Commission.

ICs must deal with complaints of cyberviolence with sensitivity and avoid trivialization and/or victim-blaming.

ICs must also be in charge of organizing awareness programmes in colleges on cyberviolence that can address what it means to interact online with sensitivity and respect.

3. Platform governance 

Platform intermediaries must ensure timely and accountable responses to complaints of gender-based cyberviolence. Global platforms with large user bases must annually publish details of the number of complaints received, subsequent action taken, use of proactive tools to flag illegal content, investment in educating users and so on.

Platform intermediaries must ensure that their content governance standards are transparent and account for women's human rights principles.

State legislation must be introduced in order to ensure that platform intermediaries have a binding duty of care to their customers. As highlighted in UK's White Paper on Online Violence, an independent regulator to ensure that companies meet this standard of care is necessary. To bring companies in line, the regulator must have the powers to penalize the company as well as senior management for violations.

The proposed amendments to the intermediary guidelines for platform companies have raised concerns about the potential for excessive censorship and surveillance because of their suggestions for automated filtering and enabling traceability. The reality of intermediary impunity and state incursion into civic liberties does present a Catch 22. However, a well-calibrated content governance regime straddling techno-design measures and legal mechanisms is a non-negotiable to protect and promote women's freedoms.

This research report was prepared under the Righting Gender Wrongs project (2018-19), a socio-legal enquiry into young women's experiences of cyberviolence.

Authors: Anita Gurumurthy, Amrita Vasudevan and Nandini Chami
Research assistance: Sarada Mahesh, Jai Vipra
Inputs: Henna Zamurd-Butt
Design and layout: Meenakshi Yadav, Ira Anjali Anwar

Research Coordination Team - IT for Change
Principal Investigator: Anita Gurumurthy
Co-investigators: Amrita Vasudevan, Nandini Chami
Research coordination: Sarada Mahesh

State Research Teams
Kerala: J.Devika (Lead), Chithira Vijayakumar, Darshana Sreedhar Mini, Resmi P.S. and Elizabeth Alexander
Karnataka: Anita Gurumurthy (Lead), Amrita Vasudevan, Nandini Chami, Sarada Mahesh, Prakriti Bakshi, Meenakshi Yadav
Tamil Nadu: Geeta Ramaseshan (Lead), Sudaroli Ramasamy, M.R.Sangeetha, S.Prabha, Nandita Krishna and Shreeja Kumar

Supported by: Web Foundation