



Executive Summary

Introduction

Digital society has transformed societal structures, with far-reaching consequences for institutional norms and practices. Social interactions online are an important aspect of this shift. While they reflect new mores coded by the technological environment, they also carry the markers of social power. The pervasive violence faced by women online is a tragic testimony to how the online public sphere and its techno-social determinants invariably entrench inequalities of the physical world.

Online gender-based violence (OGBV) – that women and people from marginal gender locations experience because of their social location and identity – is ubiquitous and takes several forms. A large body of evidence points to how victims/survivors lack recourse to accessible mechanisms for redressal. Gender-based violations online occur on privately-owned platforms that are unresponsive to the scale and pervasiveness of the problem. Even as gender equality advocates demand greater accountability from social media companies for complaints of online violence, the importance of formal systems of the law in this regard cannot be overemphasized. Judicial attitudes in cases of OGBV are an important measure of access to justice for victims/survivors; an indicator of whether those who brave the labyrinth of legal procedures feel respected and heard.

The core of addressing OGBV must rest on principles of **substantive equality** – recognizing that individuals and groups may have special needs that must be addressed to achieve equality in outcomes rather than merely formal equality, which assumes all people and groups should be treated the same way.

Dignity and **privacy**, which include aspects of personal autonomy, bodily integrity, and informational privacy, are the other cornerstones. These three attributes offer a rights-based approach to adjudicating OGBV cases. These principles were the bedrock on which this study was undertaken.

The study used legal provisions in the Indian Penal Code, 1860 (IPC), and the Information Technology Act, 2000 (IT Act), to identify cases of OGBV adjudicated in Indian courts across all levels – subordinate courts as well as High Courts and the Supreme Court. The cases, selected through purposive sampling, offer several key insights. The findings reveal how courts view cases of OGBV, flagging emerging concerns that need attention.

Findings

OGBV takes on many forms, including image-based sexual abuse, posting and uploading non-consensual intimate images and videos to social media and/or pornographic websites, voyeurism, creating fake accounts, intimidation, cyberstalking, and hateful comments. A large number of these occur on social media.

The study also captures the power relations – often fiduciary in nature – that permeate such violence. The cases reviewed reveal a recurrent pattern: older men – family members, teachers, workplace superiors – misuse fiduciary relationships, and target women and girls. The lack of autonomy in patriarchal societies makes it challenging for women and girls to confront such abuse. The analysis points to certain patterns with regard to judicial attitudes, as discussed below.

Gaps in the courts' understanding of the online public sphere

Our study of court orders in cases of OGBV shows that courts treat online violence as less serious than physical violence. This blind spot arises from an assumption that the online space is not as real or material as the physical world. What is therefore lost sight of is that online and offline spaces are, in fact, on a continuum. Our study shows that cases of online violence can lead to violence in the offline world, and vice versa. One legal provision used often in the cases in our study was criminal intimidation, where threats of non-consensual intimate image distribution (NCIID) were used to perpetrate continued physical violence. Courts, by and large, do not yet recognize gendered hate speech, gender trolling, or doxxing because of the lack of statutory recognition of these new and evolving online offenses. The upshot is that cases are filed either as defamation or other offenses, with suboptimal results for victims/survivors.

Patriarchal notions in court orders

Over the years, many studies have laid bare how courtrooms are no exception to regressive gender discourses, and do, unfortunately, legitimize sexism and misogyny. Our study also reflects this disturbing reality. While many orders are cognizant of the impact of OGBV on victims/survivors, judicial discourses are unable to transcend patronizing and protectionist tones to adopt a language centered on rights. It is also true that legal provisions in the IPC rely on tropes like “outraging the modesty of the woman”, thus lending patriarchal notions validity in courtrooms. From our sample set of cases, we observed court orders seeking to “protect” women’s alleged “modesty and chastity” from derogatory remarks online. Judgments also attributed “divinity” to women as a justification to protect them from harm. These stances are not rooted in protecting rights (such as the fundamental right to privacy) of victims/survivors, but instead rely on misplaced notions in the law that take away women’s agency and freedom as individuals.

Limited understanding of privacy in OGBV cases

The idea of privacy finds mention in some legal provisions, especially in Section 66E¹ of the IT Act, Section 509² of the IPC, and Section 354C³ of the IPC. The 2017 *Puttaswamy* verdict of the Supreme Court seems to have paved the way for OGBV cases to be viewed from a broader lens of the fundamental right to privacy of the victim/survivor in certain recent cases we reviewed. This is a positive development. However, the invocation of the victim’s/survivor’s privacy in court orders is often co-terminus with patriarchal overtones.

Expressions such as “[s]exual violence against women, apart from being a dehumanizing act, is an unlawful intrusion into the right to privacy and sanctity of a female”⁵ reveal a limited understanding of privacy. A more holistic understanding of privacy – as comprising informational, physical, and decisional autonomy – is yet to be seen in courtrooms, at least, going by our set of cases.

Procedural hurdles regarding digital evidence and inadequate focus on the online public sphere in bail orders

The requirement under Section 65B(4) of the Indian Evidence Act, 1872, for a certificate to authenticate secondary electronic evidence can often lead to evidence not being considered altogether. The cases in our study show that courts did not consider evidence not accompanied by the Section 65B(4) certificate, depriving courts of material access to evidence, and consequently, access to justice for victims/survivors.

Our study also reveals a disconcerting trend in the rationale for bail granted to accused individuals. Courts often rely on sexist and patriarchal reasoning, focusing on the complainant’s “character” rather than the alleged offense of the accused. We also observed a lack of consideration in bail conditions for the risks arising from technological aspects affecting the complainant. While general bail conditions restricting the accused from personal association with the complainant or requiring periodic reporting to law enforcement came up in the cases surveyed, specific conditions to address the online actions of the accused were absent.

Challenges in ensuring accountability of transnational social media corporations

Most cases of abuse or violence in our study occurred on Facebook, Twitter/X, and WhatsApp, and some also on Instagram, YouTube, and other websites. However, the study found that the role of such social media platforms in the dissemination and amplification of content impacting the safety and wellbeing of victims/survivors of online offenses is seldom acknowledged by courts.

In the rare instance that the courts identify the complicity of the social media platform in question, bringing the latter in as a party to the case to assist in content takedowns is not easy. The ability of national courts to mitigate harms for victims/survivors at a systemic level is, hence, limited given that social media platforms are often transnational corporations and fall beyond the territorial jurisdiction of national courts.

Way Forward

While rethinking legal-institutional responses to effectively address systemic violence online, some core concepts of the law that regulate issues of OGBV need to be questioned. The legal system, including the judiciary and the legislature, needs to take responsibility for addressing the challenges highlighted in this study. Policy changes should focus on justice and inclusivity in the digital age, capitalizing on the current consensus for effective reforms.

Global debates increasingly point to the need for platform accountability mechanisms. Liability and due diligence frameworks for business and human rights violations, including amplification of content on platforms and impacts on users, are emerging as key concerns.

While Indian courts have appointed experts to address content takedown issues in certain cases, more needs to be done to holistically tackle the larger platform ecosystem. The move to address platform regulation through the introduction of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as well as the proposed Digital India Act, which intends to replace the 23-year-old parent legislation – the Information Technology Act, 2000 – is a vital step. However, the regulatory framework requires extensive and ongoing public debate, inter alia, to also ensure that platform intermediaries with disproportionate market power can be held accountable for their duty of care towards users.

The following suggestions discuss some overarching areas to rethink approaches for courts based on this study:

1. There is an urgency to stop the trivialization of OGBV. Courts need to recognize the import of online offenses, treating them as implicating the body and personhood of the victim/survivor. This includes understanding the online-offline continuum and addressing hybrid offenses appropriately.
2. Courts must establish robust procedures for effectively addressing the online circulation of non-consensual intimate content. Courts should set down guidelines and rely on appropriate legal precedents to handle NCIID, involving privacy rights protection and recognizing emerging digital crimes. This can follow the judicial practice of recognizing systemic harms and rights of victims/survivors as seen in many pathbreaking decisions like the *Vishaka* ruling⁶ or the *NALSA* verdict.⁷ While courts have appointed experts to tackle content takedown issues, stalling the proliferation of NCIID material is an uphill task.

3. Courts should uphold victims'/survivors' right to privacy in OGBV cases, even where provisions on 'outraging the modesty of a woman' have been used. Such provisions also need revision and require consultations with women's rights groups and civil society working towards gender justice.

4. Courts should hold online platforms accountable for harmful content. They should recognize the role of social media companies in profiteering out of the viral circulation of content, and address algorithmic amplification of content that undercuts dignity and rights of users. Step change is possible only with comprehensive changes to the policy and legal regime targeting large digital corporations, including for algorithmic accountability. This is critical to move away from penalizing individual offenders and bring about systemic change for women's equal participation in the online public sphere.

5. Courts should be safe spaces for marginalized groups seeking justice. Power imbalances in interpersonal relationships due to social and cultural factors must be recognized during adjudication.

6. Procedural hurdles like certificates authenticating digital evidence should not impede justice, and bail orders should be contextualized for online spaces.

7. Ecosystem-level considerations are imperative. Sensitization within the criminal justice system, including defense lawyers and police, is crucial.

Notes:

1. Punishment for violation of privacy: Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

2. Word, gesture, or act intended to insult the modesty of a woman: Whoever, intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.

3. Voyeurism: Any man who watches, or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the perpetrator, or disseminates such image shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or subsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine.

4. *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

5. As noted in the case of *Smt. Qamar v. State of Telangana*, Bail No. 3669. (2021).

6. *Vishaka & Ors. v. State of Rajasthan*, (1997) 6 SCC 241.

7. *NALSA v. Union of India*, (2014) 5 SCC 438.

About the Report

This is the executive summary of IT for Change's research report, 'The Judiciary's Tryst with Online Gender-Based Violence: An Empirical Analysis of Indian Cases and Prevalent Judicial Attitudes.' The research was supported by the International Development Research Centre (IDRC), Canada, and the Ford Foundation. Lead authors are Malavika Rajkumar and Shreeja Sen. Scan the QR code below to access the complete report.



About IT for Change

IT for Change is a non-governmental organization that works to promote an equitable and inclusive digital society. We work with a wide range of stakeholders, using research, policy engagement, and programs in the field to further our mission. To know more, visit: <https://ITforChange.net>

