Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

FOSTERING SUSTAINABLE DEVELOPMENT THROUGH LEGAL PROTECTION FROM TECHNOLOGY-FACILITATED HARASSMENT OF WOMEN IN INDIA

SAMINA KHAN*
PhD Researcher, Faculty of Law, Universiti Kebangsaan Malaysia, Malaysia.
*Corresponding Author Email: p112584@siswa.ukm.edu.my

Dr. ROHAIDA NORDIN
Associate Professor, Faculty of Law, Universiti Kebangsaan Malaysia, Malaysia.
Email: rohaidanordin@ukm.edu.my

Dr. MUHAMAD SAYUTI HASSAN
Senior Lecturer, Faculty of Law, Universiti Kebangsaan Malaysia, Malaysia.
Email: sayutihassan@ukm.edu.my

Abstract

Technology-facilitated harassment of women (TFHW) is an escalating form of gender-based violence in digital spaces that poses a serious challenge to sustainable development, gender equality, and access to justice. This article examines the gaps and limitations in India's legal responses to TFHW, with particular reference to the country's international obligations under Sustainable Development Goal 5 (Gender Equality) and Goal 16 (Peace, Justice, and Strong Institutions). Using a qualitative legal methodology grounded in empirical research, the study draws on ten semi-structured interviews with purposively selected stakeholders. A thematic analysis of the interviews, using ATLAS.ti, revealed systemic shortcomings in legislative coverage, definitional clarity, and enforcement practices. Stakeholders identified several critical issues, including the absence of a statutory replacement for the repealed Section 66A of the Information Technology Act, the limited scope of Sections 67 and 67A, and the lack of legal recognition for non-sexual but gendered digital harms. Participants strongly advocated for a survivor-centric, harm-based, and technologically responsive legal framework that reflects the lived realities of women's digital experiences. The article argues that effective redress for TFHW requires integrated legal reform, rooted in international human rights standards and sustainable development principles. It concludes with evidence-based recommendations to strengthen legal protection and access to justice for women in India's evolving digital landscape.

Keywords: Technology-Facilitated Harassment, Cyber Law, Legal Reform, Sustainable Development, India.

1. INTRODUCTION

With internet access expanding rapidly across the globe, online spaces have become new arenas for gender-based violence. While the Internet offers opportunities for social, political, and economic engagement, it also exposes women to rising levels of abuse, intimidation, and surveillance. According to recent global estimates, nearly 85% of women have experienced or witnessed harassment in digital spaces, with disproportionately high impacts on women journalists, activists, and public figures (Economist Intelligence Unit, 2021). In India, home to one of the world's largest populations of internet users, this phenomenon is particularly concerning.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

By the end of 2025, India is projected to have over 900 million active internet users, a significant rise from the current 759 million (Kantar & IAMAI, 2022). However, the rapid digital expansion has not been matched by adequate legal and institutional safeguards for women's online safety.

Multiple studies and surveys highlight the gendered nature of digital abuse in India. A study by IT for Change found that 37% of young women surveyed in three Indian states had experienced harassment, abuse, or unwanted behaviour online, often repeatedly (Gurumurthy et al., 2019). Similarly, the Bumble (2021) survey reported that 83% of women had suffered online harassment, with one in three experiencing it weekly. Data from the National Crime Records Bureau (NCRB) reveal an 18.4% rise in overall cybercrime cases in 2019, with cybercrimes targeting women specifically increasing by 28%, while in 2020, incidents of online harassment and cyberstalking rose fivefold (ClearIAS, 2024). These alarming figures indicate a systemic failure to recognise and respond to the specific harms women face in digital spaces, perpetuating a chilling effect on their freedom of expression and access to public life.

Despite the widespread prevalence and severity of TFHW, India lacks a dedicated legal regime to address the problem. The legal framework remains fragmented and outdated, comprising primarily the Information Technology Act, 2000 (IT Act) and the newly enacted Bharatiya Nyaya Sanhita, 2023 (BNS), which replaces the Indian Penal Code (IPC). The IT Act, originally modelled on the 1997 United Nations Model Law on Electronic Commerce, was never designed to address gendered online violence (Finology, 2023). While its 2008 amendments introduced provisions such as Sections 66E, 67, and 67A to address privacy violations and "obscene" content, these provisions are narrowly construed and fail to address the full spectrum of technology-facilitated harms, particularly non-sexual but gendered abuse like doxxing, cyberstalking, deepfake threats, and misogynistic trolling (Balabantaray et al., 2023).

The repeal of Section 66A of the IT Act by the Supreme Court in Shreya Singhal v. Union of India (2015), while constitutionally necessary to safeguard free speech, also removed a provision that many law enforcement officers had relied upon, albeit problematically, to act against online abusers (Ahlawat & Sharma, 2024). In the absence of a clear statutory replacement, enforcement agencies have been forced to rely on ill-fitting provisions, such as Section 507 (anonymous threats) or Section 509 (insulting the modesty of a woman) of the IPC, now updated as Sections 354 and 79 of the BNS, respectively. These provisions, however, are not designed to address the digital nature, scale, or gendered dynamics of contemporary online abuse (Yadav & Chandel, 2020).

While the BNS, 2023 has made modest strides in criminalising online conduct, such as including cyberstalking (Section 78), revenge porn (Section 77), and digitally facilitated sexual harassment (Section 75), these reforms remain piecemeal. They do not yet constitute a coherent, gender-sensitive, and technologically attuned framework. Moreover, many critical issues such as online hate campaigns, deepfake pornography, non-consensual image dissemination, and platform accountability remain underexplored in Indian law (Sood, 2024).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

A core conceptual obstacle lies in the absence of a universally accepted legal definition of TFHW. Terms such as “cyberviolence,” “online harassment,” and “technology-facilitated gender-based violence” (TFGBV) are often used interchangeably, without legal clarity or consistency.

This definitional ambiguity obstructs enforcement, complicates case categorisation, and leaves both victims and legal actors uncertain about available remedies (NORC at the University of Chicago & International Center for Research on Women, 2022). It also inhibits comparative legal research and the formulation of global standards. Defining TFHW is not merely a semantic issue; it is foundational to establishing a targeted legal response that reflects the lived realities of women navigating digital spaces (UN Women & World Health Organization, 2023).

Beyond statutory gaps, enforcement mechanisms are often ineffective. Law enforcement agencies lack the technical training, gender sensitivity, and cyber-forensics expertise necessary to respond to TFHW (The Dialogue & Alliance for Cyber Trust and Safety, 2025).

Victims, especially those from rural or marginalised communities, often lack awareness of their rights or face systemic barriers to accessing justice. Government mechanisms such as #IamTrolledHelp have seen minimal use, and many survivors report that complaints are dismissed or minimised (IT for Change, 2018).

NGOs frequently report that women are advised to “just block the abuser” rather than pursue legal action, perpetuating a culture of impunity (Khan et al., 2023). Notably, India does not maintain disaggregated national data on TFHW, further erasing the issue from policy discourse.

TFHW also raises urgent international human rights concerns. It infringes on rights protected under the International Covenant on Civil and Political Rights (ICCPR) and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), both of which India has ratified.

It violates Article 17 of the ICCPR (right to privacy), Article 19 (freedom of expression), and contravenes Articles 2, 5, and 16 of CEDAW, which obligate states to eliminate discrimination and address structural gender inequalities. General Recommendation No. 35 of the CEDAW Committee explicitly identifies online violence as a form of gender-based violence (Committee on the Elimination of Discrimination against Women, 2017).

Furthermore, the Office of the United Nations High Commissioner for Human Rights (2022) report on privacy in the digital age highlights how online abuse, surveillance, and data misuse disproportionately affect women, exacerbating inequality and undermining autonomy, dignity, and safety.

TFHW also presents a direct challenge to India’s commitments under the Sustainable Development Goals (SDGs), particularly Goal 5 (Gender Equality) and Goal 16 (Peace, Justice, and Strong Institutions).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

Without addressing the legal and institutional blind spots that allow online abuse to flourish, these goals cannot be meaningfully achieved. A fragmented, outdated legal response to TFHW hampers access to justice, weakens institutional credibility, and restricts women's full participation in the digital and public spheres (Gurumurthy et al., 2019). This article draws on both legal analysis and qualitative insights from stakeholder interviews to critically evaluate India's legal response to TFHW.

India stands at a critical legal and ethical juncture. The unchecked spread of TFHW, in the absence of a coherent and survivor-centred legal framework, undermines constitutional guarantees and international obligations. Addressing this crisis requires more than incremental or content-based reforms. It demands a shift toward a harm-based, rights-oriented approach that centres women's lived realities, and aligns with international human rights standards and SDGs. This article contributes to that agenda by outlining context-specific, evidence-based recommendations for legal reform.

2. METHODOLOGY

This research employed a qualitative legal methodology grounded in empirical stakeholder interviews. Ten semi-structured interviews were conducted with purposively selected experts, including judges, lawyers, policymakers, NGO representatives, and an academician, to gather insights into the legal responses to TFHW in India. All interviews were conducted virtually, transcribed verbatim, and thematically analysed using ATLAS.ti software to identify key patterns, challenges, and recommendations.

Ethical clearance was obtained prior to fieldwork. To preserve confidentiality while enhancing analytical clarity, participants are referred to by stakeholder role and number (e.g., Judge 1, Policymaker 2, NGO Representative 1) throughout the findings section. This approach maintains participant anonymity without obscuring the institutional or professional lens of their insights.

The sample comprised two sitting judges, two practising lawyers, three government policymakers, two NGO representatives, and one academic expert. Participants were purposively selected based on their professional expertise and direct engagement with legal or policy issues related to TFHW in India. Interviews were conducted between January and March 2025.

3. KEY FINDINGS: STAKEHOLDER PERSPECTIVES ON LEGAL GAPS

Stakeholder interviews conducted for this study reveal a broad consensus on the inadequacy of India's current legal framework in addressing TFHW effectively. Across the judiciary, legal profession, civil society, policy sector, and academia, participants consistently emphasised that existing statutory provisions, particularly within the IT Act and the newly enacted BNS, lack the definitional clarity, gender sensitivity, and enforcement mechanisms necessary to respond to the evolving and multifaceted nature of online harms.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

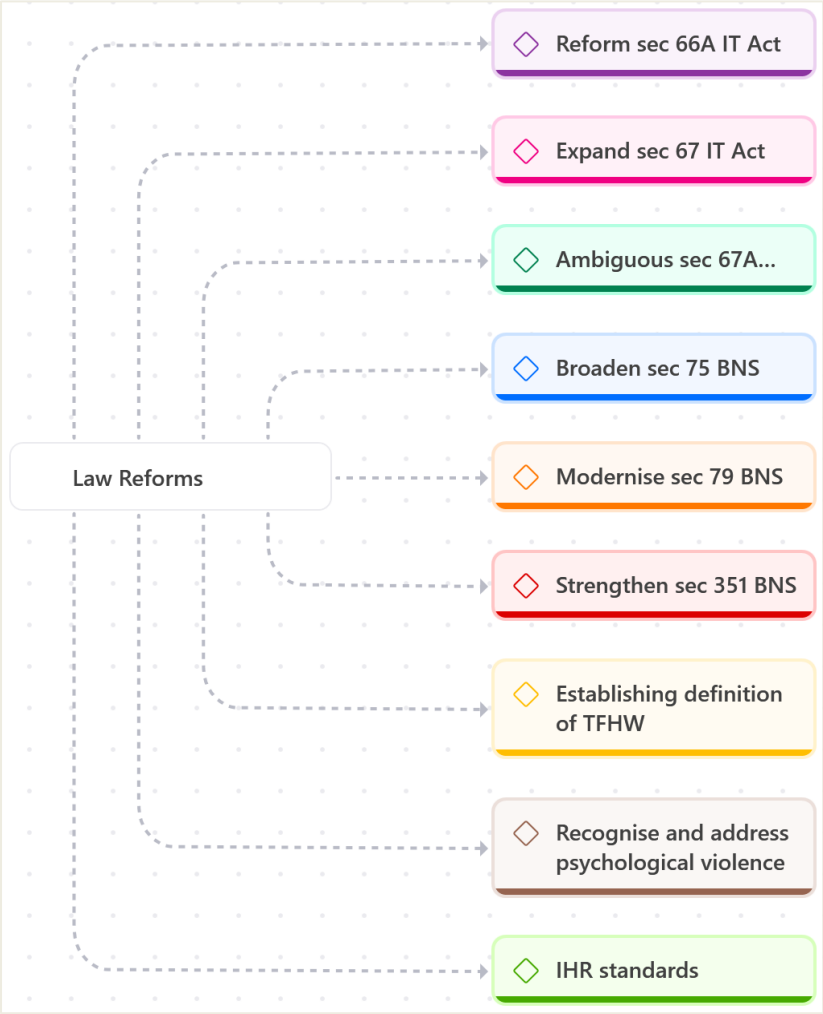

Figure 1: Law Reform Themes Identified Through Stakeholder Data Analysis

Figure 1 presents a thematic synthesis of legal reform areas derived from stakeholder interviews, visualised using ATLAS.ti software. The diagram reflects shared priorities among judges, lawyers, policymakers, academics, and NGO representatives regarding statutory amendments required to address TFHW more effectively.

The reform themes follow a logical progression, beginning with the urgent need to introduce a narrowly tailored provision to replace the repealed Section 66A, specifically targeting gendered online abuse. This is followed by calls to revise Sections 67 and 67A to clearly distinguish between consensual sexual expression and non-consensual or harmful content. Stakeholders further highlighted the importance of clarifying the extra-territorial applicability of Section 75 of the BNS.

Participants also raised serious concerns about the role and accountability of intermediaries, prompting recommendations to reform Section 79 of the BNS and amend Section 351 of the BNS to better encompass digital acts of harassment.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

Beyond individual statutory provisions, there was strong consensus on the need for a standalone legal definition of TFHW, the formal recognition of psychological violence as a punishable harm, and the alignment of Indian law with international human rights standards relating to gender-based violence, discrimination, and digital safety.

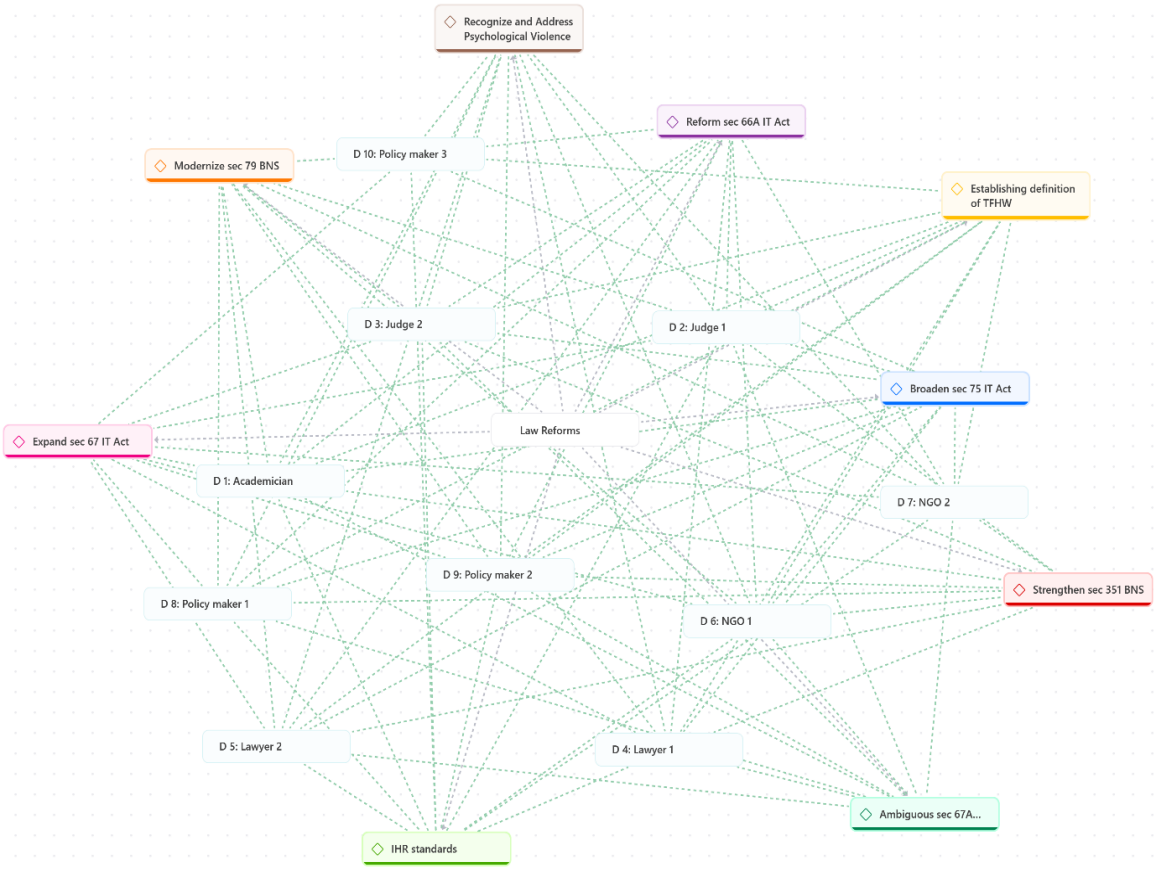

Figure 2: Stakeholders' Perspectives on Law Reforms to Address TFHW

Figure 2 visualises the network of reform themes that emerged from stakeholder interviews. The diagram illustrates how diverse professional groups are interconnected through shared concerns regarding legislative and enforcement gaps. Rather than presenting fragmented or isolated perspectives, the figure captures a clear pattern of convergence, displaying how participants across roles and sectors reinforce each other's calls for comprehensive reform. By mapping these interconnections, Figure 2 underlines the depth of cross-sectoral consensus and the collective urgency for targeted, context-sensitive legal interventions.

The thematic analysis of stakeholder interviews thus revealed a set of recurring legal gaps that expose both conceptual and procedural shortcomings within the current regulatory framework. These themes now serve as the basis for the detailed discussion that follows. The subsections below examine each reform area in turn, drawing on direct stakeholder insights to identify concrete legislative priorities.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

3.1 Reforming Section 66A of the IT Act

A central theme emerging from stakeholder interviews is the urgent need to address the legislative vacuum created by the repeal of Section 66A of the IT Act. Section 66A was declared unconstitutional in the landmark case Shreya Singhal v. Union of India (2015), as the Supreme Court found its vague and overly broad language enabled misuse and posed a serious threat to free expression. The provision was held to violate the fundamental right to freedom of speech under Article 19(1)(a) of the Indian Constitution. While the repeal was necessary to uphold constitutional principles, its absence has left a significant gap in addressing non-sexual, gendered forms of online abuse (Entertainment Desk, 2023). Stakeholders consistently noted that trolling, cyberstalking, online intimidation, and other technology-facilitated harms now fall outside the scope of existing provisions, leaving women victims with limited, meaningful legal remedies.

Judicial respondents expressed particular concern about drawing lessons from the experience with Section 66A. One judge noted:

> *Any new provision must be specific in its definitions and scope and rooted in constitutional safeguards.*

Legal professionals echoed this concern, identifying a dual challenge: while Section 66A had been overly vague and open to misuse, its repeal has resulted in a legal void. As one high court lawyer remarked:

> *Although the provision was too vague and misused, its repeal left a gap in addressing online harassment.*

Another legal respondent stressed the need for a future provision that is *"clearly defined, narrowly tailored,"* and explicitly includes harms such as cyber harassment, cyberstalking, doxxing, and deepfakes. Several interviewees also advocated for judicial oversight and stakeholder consultation in the drafting process to ensure that future legal instruments are both precise and rights-compliant.

Policymakers interviewed also acknowledged this policy vacuum. One policymaker candidly admitted:

> *We did not exactly put anything in place to specifically address online harassment after 66A was struck down.*

This statement highlights a broader institutional failure to adapt to evolving digital harms. Civil society representatives highlighted that this gap has left survivors with:

> *…very few practical legal options.*

While recognising that Section 66A had significant flaws, they emphasised that its absence has made it harder for victims to access justice. One NGO respondent argued that any new provision must be:

> *…survivor-centric and not just about punishment,*

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

calling for mechanisms that ensure platform accountability, simplify reporting, and improve police responsiveness.

The academic stakeholder also underlined the importance of adopting a rights-based, gender-sensitive approach. They stressed that a new provision should:

> *…precisely define harassment to prevent misuse,*

while also striking a balance between freedom of expression and victim protection. In addition, they recommended integrating preventive strategies such as digital literacy and algorithmic content moderation that respect privacy and user rights.

There was a broad consensus among stakeholders that the disproportionate targeting of women in digital spaces demands a legally enforceable provision that clearly addresses gendered online abuse. A survivor-centric and constitutionally sound reform would not only provide victims with more effective remedies but would also bring India's domestic framework closer to its international obligations under instruments such as the CEDAW and the ICCPR. The convergence of stakeholder views highlights the urgent need for a targeted, inclusive, and rights-aligned legislative intervention to fill the void left by the repeal of Section 66A.

3.2 Expanding the Scope of Section 67 of the IT Act

Stakeholder perspectives reveal a strong consensus that Section 67 of the IT Act is insufficient in addressing the full spectrum of TFHW. Currently, this provision penalises the publication or transmission of "obscene" content in electronic form, relying on standards of lasciviousness and prurience (Durge & Kamath, 2020). However, stakeholders emphasised that this narrow framing excludes many forms of online abuse that, while non-sexual, are deeply gendered and harmful, such as derogatory, misogynistic, or abusive remarks aimed at intimidating or demeaning women.

Judicial stakeholders highlighted this limitation. As one judge remarked:

> *Amending Section 67 to explicitly address derogatory or misogynistic content would be a meaningful step forward… Such a modification would provide clearer grounds for action, making it easier for victims to seek redress and for law enforcement to take complaints seriously.*

Another judicial participant noted that much of the harassment women face online:

> …*isn't necessarily obscene in the traditional sense,"* but is often
>
> *demeaning, threatening, or deeply misogynistic"*

and therefore, falls outside the current legal definition of obscenity.

Legal experts and civil society representatives also critiqued Section 67's limitations. They observed that the law's current language excludes a significant range of abusive behaviours that do not involve nudity or sexual content, yet nonetheless cause serious psychological, emotional, and reputational harm. The vague and outdated threshold of "obscenity" was widely criticised as inadequate for addressing modern digital abuse. As

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

a result, law enforcement agencies may be unable, or unwilling, to take action unless the content is explicitly sexual, despite the serious impact non-sexual abuse can have on women's well-being and digital participation.

Civil society actors advocated for reforms that expand Section 67 to include derogatory gender-based content and gendered hate speech. One NGO representative stressed that survivors are often retraumatized by the legal system's failure to recognise the harm they endure when such abuse is dismissed as not being "obscene enough" to warrant action. Stakeholders called for broader legal definitions that reflect the lived realities of online violence, alongside improved legal literacy among police and streamlined redress mechanisms.

Across stakeholder groups, there was strong agreement that expanding the scope of Section 67 to explicitly cover gendered, psychological, and emotional forms of abuse would enhance legal clarity, improve enforcement consistency, and strengthen protections for victims. Such a reform would acknowledge that online violence against women is not limited to sexual content but also includes gendered hate, humiliation, and silencing, forms of violence that are equally damaging and that restrict women's rights to participation, privacy, and dignity online.

3.3 Addressing Ambiguities in Section 67A of the IT Act

Stakeholders consistently identified Section 67A of the IT Act as a provision in urgent need of reform. While it criminalises the publication and transmission of sexually explicit content in electronic form, its effectiveness is severely undermined by vague and ambiguous language (Gurumurthy et al., 2018). Terms such as "sexually explicit act" and "obscene material" remain undefined within the Act, leading to inconsistent interpretations and uneven enforcement by both police and courts. Judicial participants noted that these ambiguities could result in vastly different outcomes for similar cases, depending on the discretion of the officer or judge involved. As one judge explained:

> *The current language of Section 67A can leave too much room for subjective interpretation, what one officer finds offensive, another might not.*

Legal professionals and civil society representatives echoed these concerns, pointing out that the narrow focus of the provision excludes many forms of digital gender-based abuse, including content designed to humiliate, intimidate, or threaten women. This limitation allows perpetrators to exploit legal loopholes by sharing harmful content that may not meet the traditional threshold of obscenity but nonetheless causes serious psychological harm. Lawyer stakeholders emphasised that the law must shift focus from content-based thresholds to the impact on the victim, especially in cases involving deepfakes, voyeurism, and coercive sharing of non-sexual private images.

Additionally, stakeholders observed that the provision fails to reflect the evolving nature of TFHW and the broader digital ecosystem in which it occurs. NGO representatives highlighted how women often struggle to get legal recognition for experiences of image-

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

based abuse or threatening messages unless the content qualifies as sexually explicit. An academic expert emphasised that revising Section 67A to include clear definitions, illustrative examples, and broader categories such as “objectionable” or “harmful” content would strengthen enforcement and reduce arbitrariness in prosecutions.

The findings strongly support the need to amend Section 67A to ensure legal clarity, gender sensitivity, and responsiveness to technological developments. A reformed provision should clearly define key terms, recognise non-sexualised yet abusive content, and include specific reference to harms that disproportionately affect women in digital spaces.

3.4 Broadening the Application of Section 75 of the BNS

Stakeholders expressed significant concern that Section 75 of the BNS, which replaces the former Section 354A of the IPC, remains narrowly focused on physical acts of sexual harassment and does not adequately address the increasingly complex forms of harassment occurring in digital spaces.

While the provision plays an essential role in penalising unwanted physical advances, sexually coloured remarks, and the circulation of pornographic material in workplaces or public domains, it lacks explicit recognition of non-physical and technology-facilitated forms of harassment that disproportionately target women online.

Judicial participants acknowledged the progress that Section 75 represents in updating language and penalties, but emphasised that the digital dimension of harassment remains underdeveloped in the statutory text. As one judge pointed out, although many instances of TFHW involve intimidation, persistent messaging, and reputational harm via social media, these acts are not easily captured within the current language of the provision.

Legal experts agreed, highlighting that digital harassment often manifests through repeated online intrusion, dissemination of defamatory content, or anonymous targeting, forms of abuse that fall outside the ambit of physical misconduct but have equally severe consequences for victims.

Lawyers and NGO representatives stressed that without express recognition of non-contact forms of harassment in Section 75, law enforcement officials are often reluctant to register complaints that involve online abuse.

Victims are frequently advised to pursue civil remedies or are told their experiences are not “serious enough” to merit criminal action. This institutional hesitation reinforces a hierarchy of harm that privileges physical violations over psychological or reputational abuses, thereby silencing many survivors of TFHW.

Stakeholders advocated for expanding Section 75 to explicitly criminalize both sexual and non-sexual forms of online harassment.

Such an amendment would not only ensure legal recognition of contemporary forms of abuse but would also equip law enforcement agencies with the necessary statutory backing to investigate and prosecute such offences. Importantly, participants emphasised

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

the need for gender-sensitive and survivor-centric drafting that acknowledges the impact of harassment irrespective of the medium through which it is perpetrated.

The findings suggest that broadening the scope of Section 75 to reflect digital realities is essential for bridging the legal disconnect between traditional and technology-facilitated harassment. A more inclusive provision would enhance legal access for victims, promote consistency in enforcement, and reinforce the state's obligation to protect women from all forms of gender-based violence, including those that originate or manifest online.

3.5 Modernise Section 79 of the BNS

Section 79 of the BNS, which replaces the former Section 509 of the IPC, remains rooted in a narrow conceptualisation of "modesty," failing to account for the realities of technology-facilitated harassment that disproportionately affects women in digital spaces. The provision criminalises words, gestures, or acts intended to insult a woman's modesty, but lacks the legal and conceptual scope to address violations of informational privacy and personal autonomy in the digital age (Halder & Basu, 2025).

Stakeholder interviews revealed a shared consensus on the inadequacy of Section 79's current formulation. Legal professionals and judges emphasised the need for the law to evolve in tandem with changing socio-technical realities. Judge 1 commented that:

> *Updating Section 79 BNS, aimed at addressing modern privacy concerns, is a positive step in the right direction. It recognises the evolving nature of online harassment and the need for legal provisions that reflect contemporary challenges.*

Similarly, Lawyer 2 stressed the limitations of the current statutory language and the necessity for reform:

> *To amend Section 79 BNS, especially with a clear and technology-sensitive definition of privacy violations, is a timely and necessary step. It reflects the realities of digital harassment that the existing legal framework does not adequately address.*

Further, Lawyer 1 pointed out the importance of expanding legal protection through specific recognition of digital harms:

> *Privacy violations online have evolved, and the current laws do not always cover things like doxxing, deepfake abuse, or stalking through digital means… Updating Section 79 BNS to include modern privacy threats would make it easier for victims to get protection.*

Further affirming this perspective, Policymaker 2 stated:

> *By expanding the definition to include acts such as non-consensual sharing of personal images, deepfake circulation, and unauthorised surveillance, the amendment acknowledges contemporary forms of harm not covered under traditional privacy laws.*

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

Lastly, an academic interviewee emphasised that the effectiveness of the amendment lies in its implementation:

> *Updating Section 79 BNS to address modern privacy concerns could improve legal protection against online harassment and privacy breaches… Effective enforcement and public awareness will be crucial for its success.*

These findings collectively point to an urgent need for statutory reform that reconceptualises "privacy" as a core legal interest deserving protection under criminal law. Ensuring robust protection in this regard would require not only legislative clarity but also specialised training for law enforcement, technological preparedness for investigation, and comprehensive victim-support mechanisms.

3.6 Strengthening Section 351 of the BNS

Stakeholders highlighted several limitations in the current scope and application of Section 351 of the BNS, which criminalises threats made with the intent to cause alarm, coercion, or harm. While this provision replaces Section 503 of the IPC and remains vital for addressing traditional forms of intimidation, its utility in the context of TFHW remains underdeveloped (Tripathi, 2021). Participants emphasised that the provision, in its current form, does not sufficiently account for the complexities and nuances of threats made in digital environments, particularly those that are anonymous, persistent, and amplified through social media platforms.

Judicial and legal stakeholders noted that online threats are often dismissed as non-credible due to the lack of immediate physical proximity, despite their psychological and reputational impact. As one lawyer remarked:

> *The digital space has allowed threats to evolve—not just in how they're delivered, but in the intensity of their impact.*

Anonymous messages, coordinated harassment, and indirect or implied threats can create significant fear and distress for women, yet often fall outside the prosecutorial threshold defined by existing legal language. This gap is compounded by the ambiguity surrounding what constitutes a "credible threat," which hinders both investigation and prosecution.

Law enforcement challenges were also flagged by civil society and policy stakeholders. NGO representatives pointed out that many complaints related to online intimidation are either not registered or are classified under general, less serious provisions, leading to under-enforcement. Policymakers acknowledged that Section 351 must be adapted to address the specific nature of digital threats, including those delivered through images, emojis, doctored content, or persistent tagging and surveillance. These forms of harassment, although not overtly violent, often serve as coercive tools to silence, shame, or manipulate women in online spaces.

There was strong consensus among stakeholders that reforming Section 351 to incorporate digital-specific language is essential. This includes the need for clear

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

definitions of terms such as “threat,” “intimidation,” and “alarm” within the context of online communications. Judicial participants emphasised that any amendment must also strike a balance with fundamental rights, particularly freedom of expression, in line with the constitutional principles highlighted in Shreya Singhal v. Union of India. Stakeholders advocated for narrowly tailored language that targets genuine harm while avoiding overbreadth or misuse.

Expanding Section 351 to include online threats explicitly would modernise India’s legal response to digital intimidation and provide law enforcement with clearer statutory tools. Such a reform would also affirm the state’s commitment to ensuring women’s digital safety and psychological well-being, recognising that intimidation and coercion in digital contexts are as real and harmful as those occurring offline. This would represent a critical step forward in developing a gender-sensitive and rights-based legal framework for addressing TFHW in the digital age.

3.7 Establishing a Legal Definition of TFHW

A central concern raised across stakeholder groups was the absence of a clear and standardised legal definition of TFHW within India’s legal framework. This definitional gap contributes to fragmented enforcement, legal ambiguity, and under-recognition of the wide range of gendered harms that occur online (Pandey & Shaikh, 2023). While existing provisions under the IT Act and the BNS address certain forms of cyber offences, such as stalking, voyeurism, and transmission of obscene content, none of these laws specifically define or consolidate the concept of TFHW (Kumar et al., 2021). This absence creates challenges for law enforcement, judicial authorities, and even survivors in identifying, reporting, prosecuting, and redressing acts of online harassment that are inherently gendered but not explicitly sexual or violent.

Stakeholders from the judiciary and legal profession strongly advocated for the formal incorporation of a comprehensive definition of TFHW into domestic law. One judge noted that:

> *…a well-crafted definition of TFHW can significantly contribute to the prevention and elimination of such harassment by providing a clear and comprehensive legal framework.*

Legal practitioners echoed this view, stating that the lack of definitional clarity complicates investigations and leads to inconsistent application across jurisdictions. Without a defined legal category, acts such as doxxing, deepfake threats, non-consensual sharing of personal content, and targeted character assassination are often treated as isolated incidents rather than components of systemic gender-based online violence.

Policymakers acknowledged that the legislative silence on TFHW has allowed enforcement agencies to rely on general provisions that fail to capture the unique dynamics of online abuse. As one policymaker emphasised:

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

> *Right now, the biggest problem is that TFHW isn't even clearly defined in the law... A proper legal definition would remove this confusion and ensure that all forms of digital abuse are recognised as serious offences.*

NGO representatives and academics similarly stressed that establishing a definition would not only enhance legal enforcement but also improve public awareness, advocacy, and survivor support mechanisms.

Importantly, stakeholders called for a definition that is survivor-centric, technologically current, and aligned with international standards. Such a definition should explicitly include a range of gender-based online harms, including, but not limited to, cyberstalking, non-consensual dissemination of intimate images, impersonation, online defamation, digital surveillance, and coordinated online attacks. It should also reflect the evolving nature of digital technologies and account for emerging forms of abuse, such as AI-generated non-consensual content.

The findings indicate that without a legal definition of TFHW, efforts to address online gender-based violence remain reactive, inconsistent, and incomplete. Establishing a definition would provide a foundation for developing targeted legal provisions, ensuring judicial consistency, holding platforms accountable, and empowering women to seek justice. It would also serve to operationalise India's international commitments by formally recognising digital spaces as sites of gender-based harm. A statutory definition of TFHW is therefore not only a legal necessity but also a foundational step toward developing a coherent, enforceable, and rights-based approach to online safety for women in India.

3.8 Recognising and Addressing Psychological Violence

Recognising and addressing psychological violence is essential to a comprehensive legal response to TFHW. Unlike physical violence, psychological harm, manifesting as anxiety, trauma, fear, or reputational damage, often leaves no visible scars and is frequently overlooked within India's legal framework. This is especially problematic in the context of online abuse, where violations such as doxxing, deepfake threats, and unauthorised circulation of personal data can result in significant emotional distress (Centre for International Governance Innovation, 2023). Despite this, Indian laws such as Section 66E of the IT Act and provisions under the BNS, including Sections 75 and 351, do not explicitly address psychological violence when it arises from non-sexual privacy violations or gendered abuse (Tarannum, 2023). Stakeholders consistently emphasised this gap. Judicial perspectives highlighted the emotional impact of informational privacy breaches. As Judge 1 noted:

> *Addressing psychological violence arising from the violation of informational privacy is crucial because such violations often lead to significant emotional and mental distress for victims.*

This was echoed by legal practitioners, with Lawyer 1 recalling cases involving deepfake abuse or leaked private information where victims struggled to obtain legal recourse due to the absence of visible injury or physical harm.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

Lawyer 2 reinforced the point:

> *Such violations cause significant emotional harm, including distress, anxiety, and long-term trauma*

yet they remain under-recognised in legal proceedings.

Policymakers also acknowledged the structural blind spots in current legal protections. Policymaker 1 observed that:

> *…psychological violence from privacy violations is very real, but it is often overlooked in legal cases because there is no physical harm*

suggesting that legal reform must explicitly acknowledge emotional and reputational harm. Policymaker 2 added that such harm can lead to long-term trauma and fundamentally undermine a victim's sense of security and dignity. NGO representatives similarly emphasised the debilitating effects of psychological violence, with one representative describing the emotional toll of harassment as:

> *…perpetuating a sense of insecurity*

even in the absence of overt physical threats.

This stakeholder testimony aligns with international human rights standards, which have long recognised psychological violence as a distinct form of gender-based harm. The Istanbul Convention (Article 33) explicitly requires state parties to criminalise serious psychological violence, while the CEDAW urges state parties to address all forms of violence against women, including emotional abuse facilitated by technology. As noted by the Centre for International Governance Innovation (2023), psychological impacts such as anxiety, social withdrawal, and depression are common among victims of online abuse, particularly when the abuse is prolonged, anonymous, or publicly visible, circumstances that are prevalent in digital harassment cases. The academic perspective in your study affirms the feasibility and urgency of reform. The academic expert emphasised that:

> *legal changes are feasible but challenging, requiring clear definitions of psychological harm and penalties for offenders*

and called for preventive mechanisms such as AI moderation and digital literacy programs. Stakeholders further stressed that legal change alone is insufficient: robust enforcement, judicial and police training, platform accountability, and awareness initiatives are needed to shift public and institutional attitudes. Policymaker 3 reflected:

> *People don't take psychological violence seriously... but [women] live in constant fear, anxiety, and social shame*

pointing to the systemic underestimation of emotional harm.

By explicitly recognising psychological violence, particularly when caused by digital privacy violations, as a punishable offence under Indian law, the state can bridge a significant protection gap and ensure more comprehensive safeguards for women. This

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

would not only enhance victim protection and access to justice but also align India's domestic legal framework with its obligations under CEDAW and other international human rights instruments.

4. DISCUSSION

The empirical insights gathered from stakeholders in this study underline a fundamental disconnect between India's current legal framework and the complex, evolving realities of TFHW. While various provisions under the IT Act and the BNS offer partial avenues for redress, they fall significantly short of addressing the full spectrum of gendered abuse experienced by women in digital spaces (The Dialogue, 2023). This legal inadequacy poses not only a challenge to constitutional values of dignity and equality but also directly impedes India's progress toward achieving SDGs, particularly SDG 5 and SDG 16.

The findings of this study reveal the extent to which outdated legal concepts, definitional ambiguities, and inconsistent enforcement practices continue to undermine the efficacy of existing laws (Kasturi & Dar, 2024). Survivors are often left without meaningful protection or recourse, highlighting the systemic failure of legal and institutional mechanisms to respond to the unique harms of TFHW (Mishra, 2021). In turn, this systemic gap compromises the state's capacity to uphold the rule of law in digital spaces and erodes public trust in legal institutions, an outcome directly at odds with the justice and accountability imperatives enshrined in SDG 16.

The repeal of Section 66A of the IT Act, though constitutionally justified in Shreya Singhal v. Union of India, has left a substantial legal vacuum that remains unaddressed (Bhattacharjee, 2022). Stakeholders from across the judiciary, legal profession, and civil society emphasised the urgent need for a replacement provision, one that is not only narrowly tailored and constitutionally compliant but also contextually responsive to the realities of digital violence. Harmful online behaviours such as cyberstalking, trolling, doxxing, deepfake threats, and coordinated online harassment often do not meet the thresholds of criminality established by existing statutory provisions (Sood, 2024). This legal invisibility impedes both reporting and prosecution, creating an environment of impunity that perpetuates digital gender-based violence (Gurumurthy & Dasarathy, 2022). A rights-based reform agenda must therefore incorporate this reality as central to India's broader development and gender equality commitments.

Similarly, Sections 67 and 67A of the IT Act are ill-suited to the contours of TFHW due to their narrow construction around "obscenity" and sexually explicit content (*Pramod Anandrao Dhumal v. The State of Maharashtra*, 2021). These provisions exclude a range of digital abuses that rely not on nudity but on gendered degradation, psychological intimidation, and reputational harm (Sebastian, 2023). Stakeholders advocated a decisive shift from content-based thresholds to harm-based, gender-sensitive criteria that reflect the lived experiences of survivors. Such a paradigm shift would move the law closer to recognising TFHW as a serious impediment to women's full and equal participation in public life, an outcome essential for the realisation of SDG 5.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

The BNS, while marking a step forward in terms of legal modernisation, does not fully integrate the realities of TFHW (Kumar, 2023). Provisions such as Sections 75 and 351 remain rooted in physical and traditional conceptions of threat and harm. Although Section 79 addresses cyberstalking, its limited framing, focused primarily on persistent digital pursuit, does not encompass the full spectrum of online abuse, such as coordinated trolling, gendered disinformation, or image-based harassment. As stakeholder testimony revealed, the absence of visible, physical violence leads to institutional reluctance in registering digital offences, thereby silencing victims and rendering the law inert in practice. This disconnect reflects an entrenched legal formalism that fails to keep pace with technological change, frustrating the implementation of effective and inclusive justice mechanisms envisioned under SDG 16.

Perhaps most significantly, the study's findings point to the urgent need for a comprehensive and legally binding definition of TFHW. The absence of such a definition perpetuates fragmentation across statutory provisions, leading to piecemeal enforcement, interpretive inconsistency, and a lack of institutional accountability (Kumar et al., 2021). A clear, survivor-centric definition would serve as a foundational tool for legislative, judicial, and law enforcement actors, enabling a coordinated response grounded in international human rights standards and the state's development obligations under the SDGs. Recognising TFHW as a distinct and actionable form of gender-based violence is critical to integrating digital safety within the broader human rights and development agenda.

Furthermore, stakeholder narratives affirmed the importance of embedding legal reform within real-world enforcement contexts. Legal clarity, though essential, is insufficient in isolation. As the qualitative data demonstrate, barriers to justice are compounded by institutional inertia, lack of gender-sensitive training among law enforcement, and the absence of robust accountability mechanisms for digital platforms. These multi-layered challenges highlight the necessity of a holistic reform framework that addresses both the normative and operational dimensions of TFHW.

In this regard, doctrinal legal analysis, when combined with lived professional experiences, offers valuable insights into both the structural and functional deficits of current legal frameworks (Bhagyamma, 2023). The reforms must therefore be grounded not only in legal principle but also in a practical understanding of how TFHW manifests, is (mis)handled, and is perceived by frontline legal actors. Bridging this normative-practical divide is essential if India is to uphold its constitutional and international obligations and deliver on the gender-sensitive commitments of SDG 5 and the justice-based mandates of SDG 16.

In light of these findings, the case for comprehensive, gender-sensitive, and technologically responsive legal reform is both urgent and compelling. Legal provisions must evolve to encompass the diverse and evolving harms that women face in digital environments. Moving beyond narrow interpretations of obscenity and physical harm, the legal system must adopt a framework grounded in human rights, equality, and survivor empowerment. This includes the establishment of specialised cybercrime units,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

mandatory gender-sensitivity training for enforcement agencies, and the development of institutional mechanisms that ensure timely, effective, and trauma-informed responses to digital abuse.

Ultimately, aligning domestic legal frameworks with international obligations under instruments such as the CEDAW and the ICCPR is not merely a matter of treaty compliance. It is a critical step toward fulfilling the constitutional promise of dignity, safety, and equality for women in the digital age, and a necessary condition for achieving inclusive and sustainable development, just, and gender-responsive.

5. CONCLUSION

This study highlights the urgent imperative to reform India's legal framework to effectively address TFHW, a pervasive and evolving form of gender-based violence that threatens women's rights, personal security, and digital participation. Drawing upon expert interviews with judges, lawyers, policymakers, NGO representatives, and an academician, the findings reveal that existing legislative and institutional responses remain fragmented, outdated, and insufficiently responsive to the gendered and technologically mediated nature of these harms.

The repeal of Section 66A of the IT Act, while constitutionally warranted, has left a critical legislative vacuum, particularly in addressing non-sexual but profoundly harmful digital conduct such as cyberstalking, doxxing, and online intimidation. Similarly, the narrow interpretative scope of Sections 67 and 67A, along with the limited application of relevant provisions under the BNS, fails to reflect the full complexity of digital abuse as it is experienced by women in contemporary online environments.

Stakeholders consistently called for a survivor-centric, constitutionally compliant, and technologically attuned legal approach, one that recognises the particular vulnerabilities faced by women in digital spaces. The lack of a formal legal definition of TFHW emerged as a central barrier to consistent enforcement, legal recognition, and institutional accountability. Establishing such a definition, grounded in human rights and gender equality principles, would be a foundational step toward developing a coherent, enforceable, and future-ready legal framework.

Equally critical is the integration of stakeholder perspectives into the legislative reform process to ensure that new laws are not only constitutionally sound but also responsive to real-world challenges in enforcement, access to justice, and victim protection. A holistic and forward-looking reform strategy must go beyond punitive measures to include legal clarity, enhanced institutional capacity, gender-sensitive training for enforcement personnel, platform accountability, and accessible redress mechanisms.

Importantly, these reforms must be viewed not solely as domestic legal necessities, but as integral components of India's obligations under international human rights law and its developmental commitments under the SDGs. Specifically, the pursuit of SDG 5 and SDG 16 mandates concrete legal and institutional action to eliminate all forms of gender-based violence, including those emerging in digital contexts.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

Ultimately, safeguarding women's rights in the digital age is not merely a matter of law reform; it is essential to the realisation of constitutional promises, the advancement of inclusive justice, and the fulfilment of India's vision of sustainable, equitable development. Only through comprehensive, gender-sensitive, and technologically responsive legal reform can the state meaningfully confront TFHW and contribute to building a just, inclusive, and rights-based digital society.

References

1) Ahlawat, H., & Sharma, S. (2024). Cybercrimes against women in India. ShodhKosh: Journal of Visual and Performing Arts, 5(6), 1539-1544. https://doi.org/10.29121/shodhkosh.v5.i6.2024.2430

2) Balabantaray, S. R., Mishra, M., & Pani, U. (2023). A sociological study of cybercrimes against women in India: Deciphering the causes and evaluating the impact on the victims. International Journal of Asia Pacific Studies, 19(1), 23-49. https://doi.org/10.21315/ijaps2023.19.1.2

3) Bhagyamma, G. (2023). A comparative analysis of doctrinal and non-doctrinal legal research. ILE Journal of Governance and Policy Review, 1(1), 88-94.

4) Bhattacharjee, S. (2022). Striking down of Section 66A of the IT law: The tale of a dead law. Indian Journal of Integrated Research in Law, 2(1), 1-10.

5) Bumble. (2021). Bumble India safety guide: How to identify and report online harassment. https://bumble.com/the-buzz/safety-center-bumble-india

6) Centre for International Governance Innovation. (2023). Technology-facilitated gender-based violence: Annotated bibliography on online gender-based violence [PDF]. Centre for International Governance Innovation. Retrieved from https://www.cigionline.org/static/documents/OGBV_AnnotatedBibliography_FINAL.pdf

7) ClearIAS. (2024, December 18). Cybercrime against women. https://www.clearias.com/cybercrime-against-women/

8) Committee on the Elimination of Discrimination against Women. (2017, July 26). General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19 (CEDAW/C/GC/35). United Nations.

9) Durge, M., & Kamath, K. (2020, June 30). The unconstitutionality of Section 67 of the Information Technology Act: Part I. Law School Policy Review. Retrieved from https://lawschoolpolicyreview.com/2020/06/30/the-unconstitutionality-of-section-67-of-the-information-technology-act-part/

10) Economist Intelligence Unit. (2021). Measuring the prevalence of online violence against women. Jigsaw. https://cdn.vev.design/private/WbTNgdOVVvgyq5TIBiYpWVmMCJQ2/hyw1xhPZO6_EIU_METHODOLOGY_PREVALENCE%20OF%20ONLINE%20VIOLENCE%20AGAINST%20WOMEN_FINAL.pdf.pdf?utm_medium=pr&utm_source=de-a

11) Entertainment Desk. (2023, September 13). Chinmayi Sripaada stands up for women harassed at AR Rahman's chaotic concert: "I wish you didn't have to go through sexual harassment but…". Indian Express. https://indianexpress.com/article/entertainment/tamil/chinmayi-sripaada-sexual-harassment-ar-rahman-concert-twitter-8938626/

12) Finology. (2023, June 19). Important provisions of the IT Act 2000: Safeguarding digital spaces. Finology Legal. Retrieved from https://blog.finology.in/Legal-news/it-act-2000

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

13) Gurumurthy, A., & Dasarathy, A. (2022). Profitable provocations: A study of abuse and misogynistic trolling on Twitter directed at Indian women in public-political life. IT for Change. https://itforchange.net/sites/default/files/2132/ITfC-Twitter-Report-Profitable-Provocations.pdf

14) Gurumurthy, A., Vasudevan, A., & Chami, N. (2018). Examining technology-mediated violence against women through a feminist framework: Towards appropriate legal-institutional responses in India [Discussion paper]. IT for Change. https://itforchange.net/sites/default/files/1513/ITFC-DISCUSSION-PAPER.pdf

15) Gurumurthy, A., Vasudevan, A., & Chami, N. (2019). Born digital, born free? A socio-legal study on young women's experiences of online violence in South India. IT for Change. https://itforchange.net/sites/default/files/1662/Born-Digital_Born-Free_SynthesisReport.pdf

16) Halder, D., & Basu, S. (2025). Digital dichotomies: Navigating non-consensual image-based harassment and legal challenges in India. Information & Communications Technology Law, 34(2), 163-186. https://doi.org/10.1080/13600834.2024.2408914

17) IT for Change. (2018). Submission on online violence against women to the Special Rapporteur on Violence against Women. IT for Change. Retrieved from https://itforchange.net/submission-on-online-violence-against-women-to-special-rapporteur-on-violence-against-women-1

18) Kantar, & Internet and Mobile Association of India. (2022). Internet in India 2022. https://www.iamai.in/sites/default/files/research/Internet%20in%20India%202022_Print%20version.pdf

19) Kasturi, Y., & Dar, M. A. (2024). Cybercrime in the digital age: Challenges and legal gaps in India's cybersecurity landscape. African Journal of Biomedical Research, 27(6S), 212-224.

20) Khan, S., Nordin, R., & Hassan, M. S. (2023). A routine activity approach to understanding the reasons for technology-facilitated harassment against women in India. IIUM Law Journal, 31(2), 229-252. https://doi.org/10.31436/iiumlj.v31i2.851

21) Kumar K. S., A. (2023). The Bhartiya Nyaya (Second) Sanhita 2023: An integrated perspective– A comprehensive study and analysis. Jus Corpus Law Journal, 4(2), 350-371.

22) Kumar, P., Gruzd, A., & Mai, P. (2021). Mapping out violence against women of influence on Twitter using the cyber-lifestyle routine activity theory. American Behavioral Scientist, 65(5), 689-711.

23) Mishra, A. P. (2021). A study on online violence against women during COVID-19 pandemic with special reference to India. International Journal of Law Management & Humanities, 4(6), 704-711.

24) NORC at the University of Chicago, & International Center for Research on Women. (2022). Landscape analysis of technology-facilitated gender-based violence: Findings from the Asia region. NORC; ICRW. https://pdf.usaid.gov/pdf_docs/PA00Z7GS.pdf

25) Office of the United Nations High Commissioner for Human Rights. (2022, August 4). The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights (A/HRC/51/17). UN Human Rights Council. https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age-report-united-nations-high

26) Pramod Anandrao Dhumal v. The State of Maharashtra, AIR Online Bom 35 (Bombay High Court Jan. 7, 2021).

27) Sebastian, S. (2023, October 31). Is profane language "obscene" & "sexually explicit" as per Sec. 67/67A IT Act? Supreme Court reserves judgment in 'College Romance' case. LiveLaw. https://www.livelaw.in/top-stories/tvf-web-series-college-romance-we-are-not-living-in-the-victoria-era-makers-argue-before-supreme-court-that-profane-language-does-not-fall-under-sec-67a-it-act-241284

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793323

28) Sood, A. (2024). Technology-facilitated gender-based violence in India. In R. Sinha & P. Basu (Eds.), Family and gendered violence and conflict: Pan-Continent Reach (pp. 455-475). Springer.

29) Tarannum, M. (2023). Cyber Crimes against Women in India: An analysis. Central University of Kashmir Law Review, 3(2023 issue), 133-147.

30) The Dialogue, & Alliance for Cyber Trust and Safety (ACTS). (2025). BreaktheSilo: Empirical insights into tech-facilitated gender-based violence in India (pp. 1-22). The Dialogue.

31) The Dialogue. (2023, October). BreaktheSilo: Policy framework – Streamlining gender safety in the digital space [PDF]. The Dialogue. Retrieved from https://thedialogue.co/wp-content/uploads/2023/10/BreaktheSilo-Policy-Framework.pdf

32) UN Women & World Health Organization. (2023, March). Technology-facilitated violence against women: Towards a common definition: Report of the Expert Group Meeting, 15–16 November 2022, New York, USA. UN Women. https://www.unwomen.org/en/digital-library/publications/2023/03/expert-group-meeting-report-technology-facilitated-violence-against-women

33) Yadav, S., & Chandel, S. (2020). Enactment of law for the protection of women against cybercrime. International Journal of Law Management & Humanities, 3(4), 1874-1883.