

Research Article

Digital Harassment Against Women: Need for a Gender-Sensitive Legal Framework

Sujal Chhajed*, Aman Kumar Jha and Tanishk Bhawsar

National Law Institute University, Bhopal, Madhya Pradesh 462044, India; amankumarjha.bscllb@nliu.ac.in (A. K. J.); tanishkbhawsar.bscllb@nliu.ac.in (T. B.)

* Correspondence: sujalchhajed.bscllb@nliu.ac.in (S.C.)

Abstract: Human Digital technological advancement has transformed the way women experience gender-based violence to a larger extent, that it has moved from the physical world of harassment to the almost unsecured area of the cyberspace. It is sad that apart from physical integrity, security, and participation in public, vocational, and economic activities, women's rights also face threats from cyberstalking, consensual dissemination of intimate images without endorsement, doxxing, deepfake pornography, and orchestrated online harassment. The increase in technology-enabled crime has been highlighted by the National Crime Records Bureau in India, a conclusion that has been confirmed by other surveys of which more than 50% of the women have been attacked with some kind of cyber harassment like unsolicited sexual messages, and morphed and deepfake pictures. The existing legal frameworks are however patchy: the Information Technology Act, 2000 and the (Ministry of Home Affairs 2023) which are cyber and criminal statutes respectively do not deal with the harassing act as one entity, while the Sexual Harassment of Women at Workplace which was initially created for a physical workplace is no longer relevant as it is not the real case for professional women, journalists, gig workers, and remote employees who actually work. This paper contends that the digital forms of harassment should not only be through cyber law and criminal law without these two but it must also be proponents of the issue such as occupational health and labor rights that workers suffer from more in the remote working, gig-fitness and online business exchange model where they interact and overlap. By drawing on such materials as the International Labor Organization's Violence and Harassment Convention (No. 190), the CEDAW Committee's General Recommendation No. 35, and the United Kingdom's Online Safety Act, 2023, this paper states that a gender sensitive legal framework must recognize the digital and occupational space of working women as one, uniform space, and it winds up with firm suggestions for reforming the cyber, criminal, and labor law umbrella in India's context to such an extent.

Citation: Sujal Chhajed, Tanishk Bhawsar and Aman Kumar Jha. 2026. Digital Harassment Against Women: Need for a Gender-Sensitive Legal Framework. *Digital Social Sciences* 3(2), *Digital Social Sciences* 3(2), 16-22. <https://doi.org/10.69971/dss.3.2.2026.57>

Keywords: digital harassment; cyber violence against women; gender-sensitive law; labor law; POSH Act; ILO convention 190; cyberstalking

1. Introduction

The internet was initially seen as a digital equalizer, a channel at which identity, gender and hierarchy would become nonexistent. This is a promise that has not been kept by women. Certainly, the digital spaces have turned out to be where the extant patriarchal structures are not just reproduced but are also in many ways intensified. As internet access has rapidly risen in various regions of the world, the types and severity of technology-enabled violence against women have grown accordingly – from sending unwanted sexual messages and editing images to organizing trolling campaigns, making deepfake porn, and cyberstalking.

Such a picture at the extreme is the case of India. A report from the National Crime Records Bureau, stated that there were 86,420 malware related cases reported in 2023, illustrating an increase of 30% compared to the previous year, while the rise in the rate of cybercrime was also reported. (National Crime Records Bureau 2023; Imam 2025) A considerable amount of such cases includes women as the main victims who suffered from harassment, stalking, and image-based abuse.

An often overlooked yet significant part of this issue is the connection it has with the workplace. Women, who are professionals, journalists, gig workers, and remote employees, are increasingly harassed through the use of professional email, workplace messaging platforms, video-conferencing tools, and client-facing apps which are spaces that blur the lines between “personal”



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license <https://creativecommons.org/licenses/by/4.0/>.

online life and “workplace” conduct. Mostly existing legal moves in the sectors, such as India, are based on two different solitudes existing on the agenda, that is, criminal or cyber law (the harassing act) and labor or service law (the employment relationship).

Discrimination against women through digital platforms sits in between the two desiring neither of them, alone, to be sufficient. This paper asserts that the legal framework respecting digital harassment of women needs, in a conscious way, to join criminal/cyber law with labor law recognizing that the digital and the occupational worlds, for millions of working women, have become one.

2. Conceptualizing Digital Harassment Against Women

Digital or cyber harassment against women may be understood as the use of information and communication technologies to intimidate, humiliate, monitor, silence, or control women, motivated wholly or partly by their gender. It is not a single offence but an umbrella term covering a range of conduct, including: cyberstalking (persistent, unwanted monitoring or contact through electronic means); non-consensual sharing of intimate images (commonly termed “revenge pornography”); morphing and deepfake abuse, where a woman's image is digitally altered to create sexualized or defamatory content; doxxing, or the malicious publication of private information to facilitate offline harassment; online sexual harassment through unsolicited sexual messages, images, or comments; and coordinated trolling or networked harassment, often directed at women in public life such as journalists, activists, and politicians. Research on morphed-image abuse indicates that India alone accounts for a substantial proportion of global cases involving the harassment of women through digitally altered images, frequently sexualized in nature, a trend closely associated with the growth of deepfake technology and one that leaves victims with a persistent fear of further circulation and reputational harm (Sankhala 2025).

Digital harassment is a gendered issue affecting the incidence and impact of online abuse. A recent survey highlighted the scale of the problem, which is best represented by the study of the National Commission for Women that revealed that 54.8 percent of the women surveyed mentioned the experience of some type of cyber harassment with the followed psychological implications like anxiety, fear, and reduced online safety (National Commission for Women n.d.). The Domestic Abuse Commissioner's office in the UK reported that women are twenty-seven times more likely to face this sort of harassment online than men, with a third of the total women complaining having been victims of online abuse on social media or other platforms during their lives. (Domestic Abuse Commissioner 2025)

Consequently, cyber violence can be seen as an expansion of the existing gendered relations and patriarchal policies in the digital world, not as a plastic harm. During the course of time, it is the women who live in geographies different from their employment places that follow this trend.

3. Extent of the Problem: Data and Trends

The task of quantifying digital harassment is hard by the fact that many cases of it remain unreported, there are issues with definitional inconsistency through different jurisdictions, and many national crime records do not include disaggregated data. Still, the data is quite conclusive in disclosing a continuous and increasing trend. As mentioned earlier, the NCRB's Crime in India reports have shown the rise of cyber-crime cases each year with women being majors among the victims. Old government reports had stated that the number of cyberstalking cases was 7,132 in 2016, which is 866 higher than the 6,266 cases in 2015 and 2,433 higher than the 4,699 cases in 2014, (Parahalad 2026) reflecting a gradual rise even before the surge in internet usage post-pandemic. The shift due to COVID-19 from in-person work to online learning created an expanded organizational framework of both offenders and women suffering from this kind of stress.

The incident of the gendered digital divide exacerbates the problem of risk: the more smartphones, social media, and digital financial and employment platforms facilitate women's access, the more their exposure to online abuse grows. However, this is only one side of the coin - without the introduction of parallel investments in safety infrastructure, gender-sensitive cyber-policing, and survivor-centered support services (UN Women and GSMA 2025), the equation of women's digital empowerment equals vulnerability to digital violence is all that is left on the table.

4. The Existing Legal Framework in India

4.1 Constitutional Foundations

The Constitution of India is the norm for the rights of women against electronic harassment. Article 14 assures that there is no distinct law for different people; Article 15(3) offers the opportunity of positive discrimination against women; and the Article 21 right to a life and personal liberty has been interpreted by the judiciary to include gender equality, right to privacy, bodily autonomy, etc.¹ These all are the same rights that a woman suffers from when her image, identity, or communication are used in the online world without her consent. The acknowledgment of privacy as a fundamental right gives an additional constitutional ground for regulating non-consensual image sharing and online surveillance-based harassment.

4.2 The Information Technology Act, 2000

The IT Act, 2000 is still the main cyber-law statute of India and most of its components are used in cases of digital harassment against women. Section 66E punishes (voyeurism) the appropriate profiles, publication, or transmission of a person's private area without consent; Section 67 retribution for the publication or transmission of obscene material in electronic form; Section 67A rightfully mentions the publication or transmission of sexual material; and Section 66C refers to identity theft, a problem for cases of impersonation and fake profile harassment (Information Technology Act 2000). Section 67 is likely to be the most similar as it reflects Section 292 of the old Indian Penal Code (1860), thus, extending obscenity to the digital realm as well.

The significant gap occurred due to the ruling of the Supreme Court in *Shreya Singhal v. Union of India*, which annulled Section 66A of the IT Act, the provision under which it was criminal to send “grossly offensive” or menacing electronic messages

¹ The Constitution of India, 1950 arts 14, 15(3) and 21; *KS Puttaswamy v Union of India* (2017) 10 SCC 1.

based on a finding of unconstitutional vagueness and on chilling effect to freedom of speech, which was disproportionately beyond any legitimate restriction². Although the ruling was a major victory of freedom of speech, it took away what was one of the most directly applicable provisions for online harassers and “annoyance,” allowing victims of cyberstalking and online abuse to rely on a loose patch of obscenity, voyeurism, and identity-theft provisions that do not markedly deal with harassment. Many remarked that Sections 66E, 67, and 67A were not originally meant to be anti-stalking or anti-harassment provisions, and their application in such cases is, essentially, a modification rather than the implementation of the specific provisions. (Mondaq India 2022; Legal Service India n.d.-b).

4.3 The Bharatiya Nyaya Sanhita, 2023

(Ministry of Home Affairs 2023), which is now in place instead of the Indian Penal Code, 1860, preserves the core idea of the former Section 354D IPC stalking provision that explicitly includes tracking a woman's internet use, email, or electronic communication as a way of stalking (Ministry of Home Affairs 2023; Indian kanoon 2006; Khan 2025). The BNS, too, carries forward provisions relating to sexual harassment and voyeurism analogous to the former Sections 354A and 354C IPC. Nevertheless, according to commentators, the BNS has not included any new provisions which would directly address the new forms of digital gender-based violence like deepfake pornography, algorithmically amplified harassment, or doxxing. The BNS rather leaves them for the state to deal with old laws of extension and the IT Act.

4.4 The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, for the first time in India, presents a thorough data protection scheme including the requirements for consent to process personal data and, which is important, the provisions related to children's data. (2023) Even though the Act itself does not refer to gender, its structure of consent has indirect bearing on the issue of harassment involving the unauthorized gathering, storing, or dissemination of a woman's data and images, and thus, it might be interpreted along with the IT Act's obscene and voyeurism clauses in forthcoming cases.

4.5 Judicial Responses

Though the law remains patchy, Indian courts have had a pivotal role in building the law around the issue of cyber harassment. For instance, the State of Tamil Nadu v. Suhas Katti³ case is seen as the first real conviction under the IT Act in India as the accused had made a fake email account and posted obscene things about a woman in a public Yahoo messaging group. It showed the willingness of the judicial body right from the outset that female-targeted online obscenity is no less than a serious crime. Another prominent case related to the violation of Section 67 was Aveek Sarkar v. State of West Bengal,⁴ where the Supreme Court replaced the antiquated obscene “Hicklin test” with the “community standards test” in the recent past, thereby clearing the air that content should not be deemed indecent only because they show nudity, and this rule has later been used to assess sexually altered images under Section 67.

As explained earlier, Shreya Singhal v. Union of India, has annulled Section 66A which, in effect, has remapped the boundaries of what may or may not be alleged as “offensive” conduct and consequently, not infringe upon the right of free speech.⁵ All these cases put together provide evidence of the judiciary's engagement with digital harms and, at the same time, the fact that the law has not come up with a clear rule that separates online harassment as a standalone thing.

5. The Labor Law Dimension: Digital Harassment in the World of Work

Scholarship on digital harassment has so far focused almost exclusively on the regulatory frameworks developed in the fields of criminal and cyber law, leaving out the discussion on other framings. This section argues that such an approach is unbalanced. For a vast majority of women currently working, digital harassment is not something they encounter once in a while like a criminal deed but is perceived as a regular part of their work or livelihood that they face whether it be through professional email applications, client interactions, video calls, or gig-economy apps. Given this, it is imperative that a gender-sensitive legal framework not only includes but equally highlights labor law as a parallel instrument of regulation.

5.1 The POSH Act, 2013 and the “Notional Extension” of the Workplace

The Sexual Harassment of Women at Workplace (Keche 2013; Dubey and Ananya 2013) was brought into action to validate the Supreme Court's Vishaka guidelines⁶ and is still the major labor law instrument for the workplace sexual harassment issue in India. Section 3 of the Act has made it a criminal offense to engage in sexual harassment at “any workplace,” its definition of the term “workplace” has been interpreted by the courts exceptionally broadly via the “notional extension” doctrine, it is a common understanding that harassment which is linked to work can happen outside the physical office, if there is a close relationship to work. The Delhi High Court has given the same judgment in Saurabh Kumar Mallick (this case was decided before the Act was passed but has been absorbed into the Act's interpretive framework) which is often referred to, as a basis for extending the concept of “workplace” in this way to non-traditional ones⁷. The POSH Act has a rather far-reaching coverage, personal-wise: it targets women who work regularly, temporarily, on the basis of contract, as interns, apprentices, or casual daily-wage workers, in both the organized and unorganized sectors, and as a means of compliance, whether large establishments, having ten or more employees, are set up with the Internal Complaints Committees (ICCs) or the Local Complaints Committees for smaller or informal establishments. (Dubey and Ananya 2013; PMFIAS 2025).

² *Shreya Singhal v Union of India* (2015) 5 SCC 1.

³ *State of Tamil Nadu v Suhas Katti* CC No 4680 of 2004.

⁴ *Aveek Sarkar v State of West Bengal* (2014) 4 SCC 257.

⁵ *Shreya Singhal v Union of India* (2015) 5 SCC 1.

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

⁷ *Saurabh Kumar Mallick v Comptroller & Auditor General of India* 148 (2008) DLT 289.

5.2 Work-From-Home and the Digitized Workplace

The great switch to remote work, which was a consequence of the COVID-19 pandemic, has put to the test the ideas of the POSH Act's "workplace" concept. Legal literature has come to a consensus that sexual harassment through video calls, messaging apps, or work-related social media groups would be included within the notional extension of the "workplace" by the Act, as the wording does not limit the protection to just physical facilities. (Dubey and Bhargava 2020; Bar and Bench 2020) Hence, employers have been advised to extend the POSH policy to remote and hybrid work explicitly, encompassing conduct such as misuse of inappropriate cameras, messaging, and online meeting decorum, and to adapt Internal Complaints Committee procedures by including evidence collection, virtual hearings, and confidentiality safeguards, to the remotizing context. (Sexual Harassment Law Compliance 2022)

Supporting evidence from the surveys is indicative of the extent of the issue: data from a joint survey conducted by SAFEnet and the Never Okay Project revealed that 86 of the 315 responders have been victims of sexual harassment, while working from home, (SAFEnet and Never Okay Project 2020) notwithstanding the premise that the COVID pandemic made work arrangements digital and hybrid have not reduced, and could be possible reasons for increased, women's exposure to workplace harassment.

5.3 The Gig and Platform Economy: A Regulatory Vacuum

A crucial lack of labor law regulations is at issue with women working in the gig and platform economies which include the ride-hailing, food delivery, at-home beauty and domestic services, and online freelance or "micro-task" platform work. A 2026 scoping review of gig-economy safety research found that females gig workers across ride-hailing, delivery, beauty, and platform-mediated domestic work encounter sexual harassment, verbal abuse, cyber violence, and physical threats from clients and co-workers, and are often left to their own devices like - avoiding night shifts, using location-sharing apps, carrying self-defense items - rather than getting help from the institution. (Tewari and Upma et al. 2026) Platform-level safety mechanisms like SOS buttons and GPS tracking are available but the literature states them as reactive and inconsistent application. The most important reason for this is that the platform workers are usually categorized as independent contractors, not employees, thus they are not entitled to the powers of the lawsuits like the POSH Act that are connected to an employer-employee or principal-establishment relationship, though the Act is stated to be generally wide enough. to include informal and non-traditional work arrangements. The primary outcome is hence a critical gap, as researchers have called it: no jurisdiction has yet enacted legislation that directly confronts the safety issue of women platform workers facing harassment, including on the internet and through apps, (Tewari and Upma et al. 2026; Kelly 2023; Human Rights Watch 2025) leaving this rapidly growing category of the female workforce without a recognized solution in labor law.

5.4 ILO Convention No. 190 and Recommendation No. 206

The ILO violence and harassment convention, 2019, which is the most important international instrument in this field, is the one that applies. Adopted at the Centenary Session of the International Labor Conference, and it has been in force since 25 June 2021 (International Labor Organization 2019; 2021). C190 is the first-ever international treaty to acknowledge the right to a workplace free of violence and harassment, explicitly including gender-based violence and harassment in its jurisdiction. Its approach is deliberately extensive: it encompasses all workers without regard to their contractual status, i.e., those who are unemployed, interns, volunteers, job-seekers, etc., and extends this coverage both to formal and informal, public and private sectors, as well as rural and urban areas, while the extended-definition of the "world of work" see it not just as the physical office but also as those work-related communications, including those enabled by information and communication technology. (ITF Global 2023; UNI Global Union n.d.)

In November 2025, ILO's Director-General linked the C190 with online violence and harassment against women. He described technology-assisted abuse as a force that women far from work and leadership roles; moreover, he affirmed that workers are protected both onsite, remote, or online by the observation. (International Labor Organization 2025).

Even though India has not yet ratified the ILO Convention No. 190, it may depend on its approval and the consequent adaptation of its standards in the "inclusive, integrated, and gender-responsive approach" addressing violence and harassment rights across labor and employment law, occupational safety and health law, equality and non-discrimination law, and criminal law simultaneously (International Labor Organization, n.d.), it would provide the clearest international benchmark for extending digital harassment to the workers, including those who are at present excluded from the POSH Act's practical application.

6. Comparative and International Legal Frameworks

6.1 CEDAW and General Recommendation No. 35

On the international human rights front, the Committee on the Elimination of Discrimination against Women (Committee on the Elimination of Discrimination against Women 2017) was able to adopt General Recommendation No. 35 which inter alia, updated its earlier General Recommendation No. 19 (1992) on violence against women (2017). GR 35 acknowledges that gender-based violence against women occurs in a range of contexts, both public and private, including "technology-mediated environments" and cites the "prevalent forms of violence occurring online and in other digital environments" that must be catalogued under the Convention's purview (Committee on the Elimination of Discrimination against Women 2017; UN Women 2024). This written acknowledgment carries a great weight: it makes the 189 States parties to the CEDAW to take "all appropriate measures," including legislative measures, to deal with technology-borne violence against women, (Wells and Cross et al. 2025) thus making digital harassment part of the obligations of the binding international human rights rather than treating it as a new or unregulated issue.

6.2 United Kingdom: The Online Safety Act, 2023

The Online Safety Act, 2023 of the United Kingdom establishes a statutory duty of care on user-to-user and search services across-the-board to enable persistent illegal content to be removed instantly from the sites. (Online Safety Act 2023; Domestic Abuse Commissioner UK 2025) The Act explicitly notes that such content includes priority offences such as stalking, harassment, coercive control, and intimate-image abuse. The Act makes it mandatory for Ofcom, the sector regulator, to issue the guidelines to

platforms on preventing gender dynamics that could be harmful and to carry out specific reviews of women's and girls' online harms, (Center for Countering Digital Hate 2024) which showed that they are disproportionately affected by such harms.

Platforms that become non-compliant may incur large fines up to £18 million or 10 per cent of global turnover, whichever is greater plus possible criminal liability for wrongdoers in senior management. (WeProtect Global Alliance 2023) However, critics have raised the point that a striking absence exists: content that is misogynistic, albeit not constituting a particular criminal offence, remains merely "harmful but legal," which in turn leads to a space for gender-based online abuse without clear path to regulatory enforcement. (SARSAS 2025)

6.3 European Union: The Digital Services Act

The Digital Service Act of the European Union applies comparable systemic responsibilities to online platforms in terms of the manner in which they moderate illegal content, assess risks and maintain transparency, being part of a larger issue of platform legislation as can also be seen with similar legislations in Australia and Singapore which seem to put the onus of accountability onto intermediaries for merely solving online gender-based harassment. (Apostle 2023; WeProtect Global Alliance 2024)

7. Gaps in the Current Legal Architecture

India's legal framework that caters specifically to technology-facilitated harassment still remains divided and largely reactive. The main cyber-law provisions, especially Secs. 66E, 67 and 67A of the Information Technology Act, 2000, were mainly made for privacy violations, obscenity, and sexually explicit matter only and did not cater to harassment as a separate legal right. Consequently, the users of new forms of harassment such as cyberstalking, doxxing, coordinated online harassment and deepfake-enabled abuse often find themselves restricted to analogical or indirect application of existing provisions which results in the absence of legal protection.

The issue is made worse by the circumstances after *Shreya Singhal v. Union of India*, following the decision of the Supreme Court which nullified the Section 66A of the IT Act. Even though Section 66A was criticized for its vagueness and overbreadth, and was thus, constitutionally invalidated, the deletion of it has also removed a general-purpose provision that was used to tackle some forms of offensive communication online. A specific statutory replacement has not been passed yet that would fully tackle online harassment while still meeting the constitutional requirements of clarity and proportionality.

They are also considerable lingering issues in the application of workplace safety and labor laws to new types of employment. Although the Sexual Harassment of Women at Workplace (Keche 2013) (Dubey and Ananya 2020) uses extensively broad wording that may well include informal and non-traditional work conditions, most of the operations of the act still have to rely on the presence of a recognizable employer, workplace, or Internal Committee.

GIG and platform workers, whose employment contracts are typically handled via digital mediums and don't necessarily align with the conventional employer-employee structure as per the previously defined labor law, face unique obstacles in this scenario. With regards to the absence of India's ratification of ILO Convention No. 190 and Recommendation No. 206, this represents a conspicuous void on the part of our country, which has not been able to attest to these international instruments that deal with the gender dimension in the workplace and provide violence and harassment in the world of work through an inclusive framework.

The efficacy of the current legal framework is further constrained due to gender-blind enforcement mechanisms and under-"utilization". Law-enforcement personnel limited digital literacy and training on the move are said to increase the operational gap, which is sensitive to gender issues. Additionally, there is the problem of the inconsistent implementation of the intermediary obligations and the takedown mechanisms under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which also has to do with a lack of training and specialized digital literacy among the law-enforcement personnel, and all cited above create a situation whereby some persistence social stigma occurs discouraging victims from reporting incidents and eliminating the right remedies available.

8. Towards a Gender-Sensitive Legal Framework: Recommendations

A more efficient framework should be a mix of cyberspace law, criminal law and employment law. Think about India with a specific and exceptional provision that is addressed only to zoom stalking, doxxing, and randomized bullying but is written narrowly to avoid vagueness and overbreadth which led to the invalidation of Section 66A. Deepfake-enabled sexual harassment and morphed-image abuse need to be explicitly identified in the IT Act and the Bharatiya Nyaya Sanhita and the accompanying expedited takedown mechanisms are to be rather Informational Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 per se. Cyber-crime cells and the National Cybercrime Reporting Portal should be further strengthened by extra resources, targeted training, and gender-sensitive approaches. In the area of labor, the POSH Act should be modified or clarified to clearly encompass the harassment occurring through official digital channels irrespective of the physical location of the parties.

The workers of gig platforms should be granted a grievance mechanism identical to the one provided in the POSH case, which will require platform to ensure that customers and clients have accessible mechanisms for complaints against them and other users. India should also think of lastly ratifying ILO Convention No. 190 & No. 206 and aligning domestic legislation with their integrated and gender-response approach. Furthermore, an even more effective response to technology-facilitated harassment could be achieved through the greater cooperation of Ministry of Labour and Employment, MeitY & and the Ministry of Women and Child Development, along with the regular collection of disaggregated gender data and the enforcement of stronger digital literacy and safety-by-design requirements.

9. Conclusion

Digital harassment against women is not just a problem of technology or a criminal issue; in many instances, it has become a type of work hazard that women face when they use remote work, client-facing platforms, and gig-economy applications. The legislative framework which India has at the moment is due to the IT Act, 2000, the (Ministry of Home Affairs 2023) and the POSH

Act, 2013 and it is very important, however, not complete yet. A significant void in terms of community harassment online regulations generally and regulates online harassment practically as a non-existing issue in gig and platform work, are evident in the post-Shreya Singhal situation. International instruments particularly ILO Convention No. 190 and CEDAW General Recommendation No. 35 already provide the conceptual architecture for a genuinely gender-sensitive and labour-integrated response: one that treats the digital workplace as fully within the scope of anti-harassment obligations, regardless of a worker's contractual status or the physical location from which she works. A truly gender-sensitive legal framework for digital harassment will require India, and comparable jurisdictions, to move beyond treating cyber law and labour law as separate silos, and instead build a coordinated architecture that follows women across the full range of spaces physical and digital, formal and informal in which they now live and work.

References

- Apostle, Julia. 2023. The UK's Online Safety Act and EU's Digital Services Act: What Online Service Providers Should Know. *Orrick*. <https://www.orrick.com/en/Insights/2023/11/The-UKs-Online-Safety-Act-and-EUs-Digital-Services-Act-What-Online-Service-Providers-Should-Know>
- Bar and Bench. 2020. 'The Dynamic Workplace in a Work from Home Era.' *Bar and Bench*. <https://www.barandbench.com/columns/the-dynamic-workplace-in-a-work-from-home-era-operation-of-the-sexual-harassment-of-women-at-workplace-act-2013>
- Center for Countering Digital Hate. 2024. 'The UK's Online Safety Act: A Year On.' *Center for Countering Digital Hate*. <https://counterhate.com/blog/the-uk-online-safety-act-a-year-on/>
- Committee on the Elimination of Discrimination against Women. 2017. 'General Recommendation No 35 on Gender-Based Violence against Women, Updating General Recommendation No 19.' *United Nations Digital Library*. <https://digitallibrary.un.org/record/1305057?ln=en&v=pdf>
- Domestic Abuse Commissioner. 2025. We Must Build on the Online Safety Act to Ensure All Victims Are Protected from Online Abuse. *Domestic Abuse Commissioner*. <https://www.domesticabusecommissioner.uk/we-must-build-on-the-online-safety-act-to-ensure-all-victims-are-protected-from-online-abuse/>
- Dubey, Bhumitra, and Ananya Bhargava. 2020. Applicability of the POSH Act, 2013 in Remote Working or Working from Home. *iPleaders*. <https://blog.iplayers.in/applicability-posh-act-2013-remote-working-working-home/>
- Human Rights Watch. 2025. The Gig Trap: Algorithmic, Wage and Labor Exploitation in Platform Work in the US. *Human Rights Watch*. <https://www.hrw.org/report/2025/05/12/the-gig-trap/algorithmic-wage-and-labor-exploitation-in-platform-work-in-the-us>
- Imam, Mahira. 2025. Conceptualising Cyber-Crime Against Women: Beyond Numbers and Online Misbehaviour. *Impact and Policy Research Institute*. https://www.impriindia.com/insights/cyber-crime-against-women/#google_vignette
- India Code. 2000. Information Technology Act, 2000 (21 of 2000). *India Code*. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- Indian kanoon. 2006. Indian Penal Code, 1860 (45 of 1860). *Indian kanoon*. <https://indiankanoon.org/doc/1569253/>
- International Labour Organization. 2019. Eliminating Violence and Harassment in the World of Work: Convention No 190, Recommendation No 206 and the Accompanying Resolution. *International Labour Organization*. <https://share.google/11ZIBNf0EIJasmn82>
- International Labour Organization. 2019. Violence and Harassment Convention 2019 (No 190). *International Labour Organization*. https://normlex.ilo.org/dyn/nrmlx_en/f?p=NORMLEXPUB:12100:0::NO::P12100_INSTRUMENT_ID:3999810
- International Labour Organization. 2021. Violence and Harassment in the World of Work: A Guide on Convention No 190 and Recommendation No 206. *International Labour Organization*. <https://www.ilo.org/publications/violence-and-harassment-world-work-guide-convention-no-190-and>
- International Labour Organization. 2025. Protecting Women from Violence in the Digital World of Work. *International Labour Organization*. <https://www.ilo.org/resource/statement/protecting-women-violence-digital-world-work>
- ITF Global. 2023. ILO Convention 190.
- Keche, Urwi. 2013. Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013. *Slideshare*. <https://www.slideshare.net/slideshow/sexual-harassment-of-women-at-workplace-prevention-prohibition-and-redressal-act-2013/236034761>
- Kelly, Phillipa. 2023. So Many Reports of Violence and Abuse: How the Gig Economy Fails Women Around the World. *Center for Business and Human Rights*. <https://www.business-human-rights.org/ru/%D1%81%D0%B2%D0%B5%D0%B6%D0%B8%D0%B5-%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/so-many-reports-of-violence-and-abuse-how-the-gig-economy-fails-women-around-the-world/>
- Khan, Mohd Shadique. 2025. Online Harassment of Women: Legal Recognition and Gaps in Indian Cyber Laws. *LegalCyfle*. <https://legalcyfle.in/online-harassment-of-women-legal-recognition-and-gaps-in-indian-cyber-laws>
- Legal Service India. n.d. Cyber Stalking: A Menace for Women. *Legal Service India*. <https://www.legalserviceindia.com/legal-article-11444-cyber-stalking-a-menace-for-women.html>
- Ministry of Electronics and Information Technology. 2024. Digital Personal Data Protection Act, 2023 (No. 22 of 2023). *Ministry of Electronics and Information Technology*. <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>

- Ministry of Home Affairs. 2023. Bharatiya Nyaya Sanhita, 2023 (45 of 2023). *Ministry of Home Affairs*. https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf
- Mondaq India. 2022. Cyberstalking and the Indian Jurisprudence. *Mondaq India*. <https://www.mondaq.com/india/social-media/1193320/cyberstalking-and-the-indian-jurisprudence>
- National Commission for Women. n.d. Cyber Crimes Against Women in India. <https://www.scribd.com/document/815135407/paper-1>
- National Crime Records Bureau. 2023. Crime in India 2023. *National Crime Records Bureau*. <https://www.ncrb.gov.in/crime-in-india-year-wise.html?year=2023&keyword=>
- Online Safety Act 2023, c 50 (UK).
- PMFIAS. 2025. Prevention of Sexual Harassment (POSH) Act. *PMFIAS*. <https://www.pmfias.com/posh-act/>
- Prahalad, Revindra Kumar and Grupreet Singh. legal Service India. 2026. Cyber Stalking and Harassment on Women in India: A legal study. Zenodo. <https://zenodo.org/records/21308910>
- SAFEnet and Never Okay Project. 2020. Applicability of the POSH Act, 2013 in Remote Working or Working from Home. *iPleaders*. <https://blog.iplayers.in/applicability-posh-act-2013-remote-working-working-home/>
- Sankhala, Layan. 2025. Digital Victimization of Women in Cyberworld. *International Journal for Research Trends and Innovation* 10: 1-31. <https://www.ijrti.org/papers/IJRTI2503099.pdf>
- SARSAS. 2025. Online Safety Act 2023: What Protections Are There for Women and Girls? (Part 2). *SARSAS*. <https://www.sarsas.org.uk/online-safety-act-2023-what-protections-are-there-for-women-and-girls-part-2/>
- Sexual Harassment Law Compliance. 2022. 'Work from Home.' https://doe.gov.in/files/inline-documents/DoE_Prevention_sexual_harassment.pdf
- Tewari, Deeksha Bajpai, Upma Gautam, Ankita Mishra, Kanishka Verma, Vaishnavi Jaiswal and Priya Das. 2026. Strategizing Safety for Women in the Gig Economy: A Scoping Review of Policy Research. *Frontiers in Organizational Psychology* 4:1-22. <https://doi.org/10.3389/forgp.2026.1838133>
- UN Women and GSMA. 2025. Data cited in IMPRI Impact and Policy Research Institute, 'Conceptualising Cyber-Crime Against Women: Beyond Numbers and "Online Misbehaviour.'
- UN Women. 2024. Technology-Facilitated Gender-Based Violence: Developing a Shared Research Agenda. *UN Women*. <https://www.unwomen.org/en/digital-library/publications/2024/09/technology-facilitated-gender-based-violence-developing-a-shared-research-agenda>
- UNI Global Union. n.d. Training Guide for Trade Unions on ILO Convention 190.
- Wells, Mikaela, Cross Conrad, and Karson Taylor. 2025. The Regulatory Review. 2025. International Solutions to Technology-Facilitated Gender-Based Violence. <https://www.theregreview.org/2025/01/18/seminar-international-solutions-to-technology-facilitated-gender-based-violence/>
- WeProtect Global Alliance. 2024. Policy Briefing: UK Online Safety Act. <https://www.weprotect.org/wp-content/uploads/UK-Online-Safety-Act-Policy-Briefing.pdf>