"Sexual Harassment in the Digital Workplace: Gaps in POSH Act and the Need for Legislative Reform"

By Author

K .Dharshini

BBALLB (HONS)

ABSTRACT

The rise in sexual harassment on digital platforms due to the work-from-home mode has highlighted the inadequacies in India's POSH Act of 2013, which predates the use of virtual means of interaction, such as video conferencing, emails, and instant messaging applications. The definition of 'workplace' and harassment in the Act encompasses verbal and non-verbal acts of misconduct, but there is no clear provision for digital forensic investigations, virtual harassment, and algorithmic harassment, making enforcement problematic.

Although judicial interpretations of the law through the Vishaka guidelines have been beneficial, concerns remain regarding the exclusion of non-women complainants, conciliation as a coercive process, and lack of adherence by small and medium enterprises, requiring reforms such as mandating digital compliance, extending the period for complaints, and formulating virtual-specific policies.

This study discusses the inadequacy of the POSH Act in dealing with sexual harassment within the realm of digital and virtual workplace environments. The analysis centers on the limited scope of the 'workplace' term defined in Section 2(o) of the Act. It asserts that since the term 'workplace' is not explicitly expanded to cover virtual workplace environments, the POSH Act is inadequate to deal with sexual harassment in the current digital age. It also reveals that there is no uniform procedure established by the POSH Act for dealing with digital evidence.

INTRODUCTION

While the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (POSH Act), was a landmark legislation in India in addressing workplace harassment in line with the Vishaka guidelines, which emphasized provision of a safe environment for women, the advent of digital work culture in India due to the COVID-19 pandemic has exposed significant gaps in its legislative framework when it comes to addressing harassment through emails, video calls, messaging applications, and other virtual mediums.

Issues with Digital Workplace: The traditional understanding of the terms ‘workplace’, ‘employer’, and ‘course of employment’ used in the POSH Act fails to apply to hybrid or completely remote work scenarios, leading to vulnerability among gig workers, freelancers, and other employees working through platforms. Forms of

digital harassment such as unwelcome video intrusion and bias created by algorithms during virtual interactions cannot be clearly defined and collected as evidence for use before ICCs.

Legislative Shortcomings:The POSH Act does not contain any provisions dealing with harassment in virtual spaces, online evidence-gathering, or legal responsibility towards non-conventional employers (gig platforms). Even after the Government confirmed in 2020 that POSH applies to remote work situations, it fails to incorporate the same into the Act. Compliance remains weak, especially in the case of SMEs and LCCs.

Legislative Reforms :Immediate reforms are required to redefine critical terms, provide penalties related to turnover, and incorporate digital conduct guidelines into POSH, along with incorporating digital redress mechanisms like SHe-Box portals.

EVOLUTION OF WORKPLACE UNDER POSH ACT

The POSH Act of 2013, which stands for Prevention of Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal), introduced revolutionary amendments into what constitutes the "workplace," as traditionally understood. It not only included geographical spaces but also incorporated virtual spaces wherein a woman worked in any capacity whatsoever. From an initial conceptualization that was limited to workspaces within offices and factories, the text of the POSH Act has been reinterpreted over time to include work-from-home conditions, commute journeys, client offices, and even online conference calls, despite many digital-era lacunae.

Workplace in the conventional sense under POSH Act

"Workplace" under the POSH Act includes:

- Work premises where the employee generally works, such as departmental or project office.
- Premises visited by the employee in relation to her work, such as client offices, hotels, or transport used for the purpose of carrying out work-related tasks.
- Organized as well as unorganized sectors, including NGOs, cooperative societies, self-employed women, and even home-based workers to some extent.

Over time, the interpretation of the workplace became that of a "space of power" and not a mere geographical space because of the emphasis on the functional execution of the employment relationship.

EMERGENCE OF VIRTUAL WORKPLACE

. In the context of telecommuting, virtual teams, and digital tools, much debate has arisen on whether the Act will apply in cases of harassment carried out on:

videoconferencing software (Zoom calls/meetings, virtual training).

instant messaging services like WhatsApp, Slack, and Teams, and email communications.

the virtual client platform and the interface used by freelancers/contractors/gig workers.

Some legal opinions indicate that the term "workplace," as used under the POSH Act, could be interpreted liberally enough to cover these virtual work environments, in the sense that the harassment takes place "at the workplace" as a result of the employment relationship and while communicating in work-related matters. Yet, the Act does not specifically mention either "digital workplace" or "cyber-workspace."

FORMS OF DIGITAL SEXUAL HARRASMENT

Digital sexual harassment at the workplace involves unwanted sexual behavior using digital media (e.g., email, chat, video conferencing, social media, etc.) in the workplace that results in a hostile and intimidating work environment. The key types include:

1.Inappropriate digital communications

Sending sexually offensive texts, emails, or chat messages; frequently making sexual jokes, using emojis, asking inappropriate sexual questions, etc.

2.Explicit material sent through digital media

Forwarding pornographic images, videos, or website links within work-related WhatsApp groups or mailing lists or sending unsolicited nude pictures or cyber-flashing during work-related digital communications.

3.Making sexist or sexual comments during virtual meetings

Saying offensive things regarding a person's body, dressing up, or personal appearance during video conferencing or telecommunication.

4.Non-consensual transmission of intimate digital photos or videos

Transmitting or threatening to do so any private photos or videos without prior permission from an individual (revenge porn or sextortion).

5.Stalking or excessive surveillance using digital media

Persistently stalking, surveilling, or monitoring someone's online activities or contacting them excessively and continuously outside their working hours even after being told not to do so.

6.Blackmail through digital media

Making threats or pressuring a person into sending nude pictures or having explicit sexual conversations.

7. Bullying or cyber mobbing

Employing any online forum to mock the individual based on their sexual activity or organising other people from work or outside to send sexual threats or memes.

AMBIGUITIES IN APPLICATION TO VIRTUAL PLATFORMS UNDER THE POSH ACT

While the POSH Act, 2013 (Sexual Harassment of Women at Workplace Act) focuses mainly on workplaces in physical spaces, several ambiguities arise when the act is applied to virtual or digital platforms, such as e-mails, WhatsApp, Zoom calls, and other social networking sites which are used by the workers during their professional duties. Several cases, including Dr. Amit Kumar v. University of Delhi, by Delhi High Court, in 2025, have interpreted workplace to include virtual platforms for working purposes; however, there are no special sections or clauses in the POSH Act for addressing ambiguities concerning digital or remote/hybrid working systems, including the issues of algorithmic harassment and confusion between personal and professional digital activities (like on Slack or Facebook).

EVIDENCE GATHERING AND TECHNOLGICAL CHALLENGES

Evidence-gathering in digital sexual harassment cases is seriously complicated by the fragile, easily altered nature of electronic records, such as deleted or self-destructing messages, edited screenshots, and un-backed-up chats across platforms like WhatsApp, Teams, or email. The ephemeral design of some apps (e.g., disappearing messages) makes it difficult to capture reliable, contemporaneous proof before it vanishes.

Technologically, investigators face huge volumes of scattered data—emails, chat logs, cloud files, and video-call recordings—often spread across personal and work devices, with platform-specific privacy settings that restrict access or exports. Properly preserving this data requires forensic-grade handling: maintaining chain-of-custody, capturing metadata (time stamps, sender-receiver IDs, IP traces), and ensuring authenticity under Section 65B of the Indian Evidence Act.

In practice, most workplaces lack clear internal protocols, standardised tools, or trained personnel for digital forensics, leading to ad-hoc collection, loss of critical evidence, or inadmissible material in POSH or criminal proceedings. Without structured mechanisms for early-stage digital evidence preservation, victims struggle to prove repeated or coordinated harassment that occurs largely in virtual spaces.

DATA PRIVACY, SURVEILLANCE, AND DIGITAL MONITORING

There are several privacy, surveillance, and digital monitoring issues associated with workplace environments where employees can be subject to various forms of tracking including usage of software such as keystroke loggers, cameras, monitoring apps that track an individual's activity online continuously, among others. It should be noted that the use of such instruments can be considered intruding even further when considering the fact that employees might do their job remotely or use their own personal equipment, such as a phone, thus giving access to more sensitive personal information.

The situation becomes more complicated in India where there is no clear-cut approach concerning data privacy, which includes having a digital workplace. Also, in India, there is much room left for surveillance, as well as exemptions to surveillance under the law for purposes of national security. Additionally, employees will find it difficult to control how data they provide will be used by their company, which may result in retaining logs, screen recordings, and location data unnecessarily and without any consent.

Regarding sexual harassment, unnecessary monitoring can lead to discouraging victims from reporting abuse.

CURRENT LEGAL AND POLICY RESPONSES

Current efforts in India to combat digital sexual harassment through existing laws and policies seem fragmented and reactionary rather than completely customized to the digital workspace. This is primarily based on the main framework of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, which defines any form of "unwelcome sexual conduct" as harassment, which includes digital interactions, and obligates the employer to protect the employees from harassment and initiate internal investigation against sexual harassment in the workplace.

Along with the POSH Act, other laws like the Information Technology (IT) Act, 2000 (Amendment) prohibit cyberstalking, non-consensual circulation of private photographs (Section 66E) and the transmission of obscene or sexually explicit material (Sections 67/67A). Other provisions include criminal intimidation, stalking and defamation, which may result from cyber-coercion. In reality, there is a lack of implementation, under-reporting and a failure to report online abuse under the criminal provision.

Regarding the issue of privacy and employee monitoring, the Digital Personal Data Protection Act, 2023 (DPDP) and the fundamental right to privacy necessitate that any form of employee surveillance should adhere to transparency, purpose limitation, and data retention practices.

However, many employers use these technologies without having any relevant policies or even informed consent from employees, which results in a grey area where there is a thin line between legitimate supervision and invasive activities on the personal privacy of employees.

On the policy front, the increasing emphasis on compliance with labour and POSH guidelines calls for revisiting internal policies regarding remote and digital workplaces, the permitted use of communication technology, and procedures for handling digital evidence. These are still at the advice stage rather than a statutory requirement, so there are several routes to seek legal recourse for digital harassment cases, but the system lacks a unified approach under the POSH framework

COMPARATIVE AND INTERNATIONAL LESSONS

. Experience from comparative analysis and internationally reveals that effective strategies against digital sexual harassment involve a combination of legal recognition of harassment activities, protective measures for data security, and work policy guidelines. A number of European nations recognize digital harassment and stalking as criminal acts within their laws on gender-based violence, including the Istanbul Convention, while simultaneously imposing restrictions on workplace surveillance by employees through the General Data Protection Regulation (GDPR) and domestic employment laws.

Meanwhile, other legal frameworks such as those within some Australian and American states have enacted explicit statutory offences of "image-based abuse" and threatening to publish intimate images (similar to "revenge porn" or sextortion) that may be used as part of a digital harassment claim. Digital safety charters and governance approaches to online platforms have focused on transparency and risk-based content moderation practices, reporting procedures, and appeal mechanisms that should be applied in the workplace-specific context.

The key lessons learned that could be transferred to India would be to:

Modify the POSH regime (and its subordinate rules) to provide an explicit definition of digital harassment, and obligations on virtual workplaces, rather than depending exclusively on judicial interpretation;

Make POSH-related internal company policies meet GDPR-like principles of transparency, purpose limitation, and data minimization when monitoring remote working environments; and

Enact specific criminal-law provisions targeting non-consensual image publication or sextortion based on modern overseas legislation.

PROPOSED LEGISLATIVE AND POLICY REFORMS

The POSH legislation and policy changes suggested for digital sexual harassment in India need to address critical gaps in the POSH act by making the POSH legislation compliant with cyber law and data protection principles. Amendments in the POSH legislation are required, making sure that "digital sexual harassment" has been recognized, and the usage of email, chats, video calls, and social media use related to work comes under the ambit of the "workplace." Although courts have defined the term very broadly, clarity on legal grounds would make the job easier for the Internal Committee.

Some kind of digital evidence protocol needs to be devised especially for the POSH complaint to standardize the methods used to preserve screen shots, chats, metadata, and video call recordings according to Section 65B of the Indian Evidence Act and provide the required assistance to ICs from the employers' end. Amending cyber criminal laws is required, which will include provisions of non-consensual image-sharing, deep fakes, and sextortion.

According to the 2023 Digital Personal Data Protection Act, it is necessary to establish guidelines that will minimize the extent of invasive surveillance, such as non-stop webcam tracking, while ensuring that the minimum amount of personal information be collected in the course of conducting POSH investigations. It is necessary to compel businesses to review their POSH policies in the context of the digital work environment and lay down strict guidelines concerning the use of communication services and the availability of digital harassment training programs.

CONCLUSION

Sexual harassment in the digital realm in the workplace highlights significant weaknesses in the current Indian legislative structure and policy, wherein the POHA is disconnected from other laws such as cyber and data protection laws. Despite the courts beginning to recognize virtual spaces as part of the workplace environment, there has been inconsistent implementation of the law, low reporting rates, and confusion surrounding what constitutes harassment.

As workplaces evolve into more remote and platform-based settings, it is necessary for India to adopt a holistic approach to the issue of online sexual violence at the workplace, anchored on the POHA and incorporating provisions addressing digital sexual abuse, evidence for digital offenses, and criminal sanctions against image-based abuse and sextortion.

At the same time, monitoring practices in workplace settings should be subject to strict guidelines on the handling of data and information privacy issues.

Through a coordinated effort that combines criminal, data, and labor compliance legislation in a gender-conscious and technology-aware manner, digital harassment can be combatted more effectively. Only in such a way will workplaces in the digital sphere become secure environments free from harassment.

KEY SUGGESTIONS

An important recommendation would be to modify the POSH act and the accompanying regulations to specifically address the issues of “digital sexual harassment” and virtual workspaces and connect them to the Digital Personal Data Protection Act, 2023 and enhanced cyber-crime laws. It may be recommended that employers create internal guidelines with respect to POSH policy for remote work that should contain information about acceptable usage of messaging applications, process of reporting online harassment and digital evidence preservation techniques.

The training modules for the Internal Committees, Managers and HR professionals should include digital harassment cases, concept of digital consent, and the procedure for evidence gathering from online communications. Finally, there should be put in place a dedicated digital redressal procedure based on She-Box which would allow for integrating complaints, e-evidence filing, and coordination with cyber cells.