Decoding Workplace Sexual Harassment through Digital Forensics

Kana Mukherjee
Professor, Department of Legal Science
Techno India University

and

Kalyani Bhowmick
Research Scholar, Department of Legal Science
Techno India University
kb2509@gmail.com

https://doi.org/10.5281/zenodo.21900916

ABSTRACT

The rapid digitisation of workplace communication has transformed the manner in which sexual harassment occurs, is reported and is investigated. Interactions now leave persistent traces in emails, chat logs, access records, metadata and social media, making electronic evidence central to inquiries under the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (POSH Act). This article examines the intersection between digital forensics and workplace sexual harassment investigations in India. Adopting a doctrinal and analytical methodology, it explores how Internal Committees may utilise digital evidence while complying with the principles of natural justice, privacy rights and data protection obligations.

The article identifies key challenges, including the authenticity of digital evidence, risks of manipulation and deepfake fabrication, chain-of-custody concerns, cross-border data access, and the absence of forensic expertise within Internal Committees. It then proposes a structured framework for the collection, preservation, analysis and presentation of electronic evidence in POSH proceedings. The study argues that the effectiveness of the POSH regime will increasingly depend upon the capacity of organisations and Internal Committees to deploy forensic tools responsibly, and advocates specialised training, forensic readiness and robust digital evidence management protocols as essential components of contemporary workplace governance.

KEYWORDS: POSH Act, Workplace Sexual Harassment, Digital Forensics, Electronic Evidence, Internal Committee, Cyber Investigation, Data Privacy, Bharatiya Sakshya Adhiniyam, Workplace Compliance, Artificial Intelligence.

Introduction

The Role of digital Forensics : Turning conflicting stories into provable facts

In the age of smartphones, cloud computing and online interactions, the digital world records nearly everything. Whether it's a late-night text message, a calendar entry, an email headers or a social media post, digital breadcrumbs are constantly being left behind.

Digital Forensics is the science of identifying, preserving, analyzing and presenting digital evidence in a way that is legally sound. It is no longer a niche specialty used only in cybercrime cases. It has become indispensable in civil disputes, workplace misconduct, defamation claims and sexual harassment allegations.

In the he-said, she-said scenarios, where two people offer starkly different versions of events, the absence of physical evidence once stalled investigations. But digital forensics changes that. It allows investigators to shift from ambiguity to clarity by examining the following:

1. Metadata: Information hidden inside files, such as timestamps, authorship and device information, which helps verify authenticity
2. Hashing : A technique that ensures digital evidence has not been tampered with
3. Email Header Analysis- Reveals the real origin and routing path of emails, cutting through forgery claims
4. Geo-location Data – determines who was where and when
5. Log Files – Reconstruct timelines of system usage, access history and user behavior
6. Deleted File Recovery – Retrieves erased messages or files, potentially reviving forgotten truths
7. Data Analysis Patterns – Tracks harassment or misconduct across messaging apps, emails and cloud tools

These methods complement traditional approaches like interviews and physical inspections. They help establish a chain of events, validate or challenge allegations and ensure fair outcomes, even when emotions run high and facts seems buried.

Of course, challenges persist. Encrypted files, refusal to share devices, deepfakes or anonymous communication can complicate investigations. But even in such cases, digital forensics often provides tools to bypass barriers or trace anomalies.

Research Methodology

Research Design

This study adopts a qualitative and doctrinal legal research methodology to examine the role of digital forensics in the investigation of workplace sexual harassment complaints under the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 ("POSH Act"). The research is exploratory and analytical in nature, seeking to understand how digital forensic techniques can enhance the effectiveness, fairness, and reliability of workplace harassment investigations in the contemporary digital environment.

Sources of Data

The study is primarily based on secondary data collected from a wide range of legal, technological, and academic sources, including:

1. Statutory provisions such as the POSH Act, 2013, the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, and relevant data protection and privacy regulations.[1]
2. Judicial decisions of the Supreme Court of India, High Courts, and relevant international jurisprudence concerning electronic evidence, workplace harassment, privacy rights, and digital investigations.
3. Government notifications, guidelines, reports, and policy documents issued by the Ministry of Women and Child Development, Ministry of Electronics and Information Technology, and other regulatory authorities.
4. Scholarly literature comprising peer-reviewed journal articles, books, conference papers, and research reports relating to digital forensics, cyber investigations, electronic evidence, workplace governance, and sexual harassment law.
5. Technical publications and industry best-practice frameworks issued by digital forensic organisations, cybersecurity agencies, and professional investigative bodies.[2]

Research Approach

The study employs doctrinal analysis to examine the legal framework governing workplace sexual harassment investigations and the admissibility of electronic evidence. A comparative analytical approach is also utilised to evaluate established digital forensic methodologies and assess their suitability within the procedural framework of Internal Committee inquiries.

In addition, the research adopts a problem-solution approach by identifying practical challenges faced during workplace harassment investigations, including evidence authenticity, data manipulation, privacy concerns, chain-of-custody issues, cross-border data access, and the lack of forensic expertise among Internal Committees. These challenges are subsequently analysed to develop a structured digital forensic investigation framework.

Scenario-Based Analysis

To demonstrate the practical application of digital forensic techniques, the study incorporates illustrative workplace harassment scenarios involving emails, instant messaging applications, social media platforms, cloud-based collaboration tools, CCTV footage, geolocation records, wearable devices, and multimedia evidence. These scenarios are used solely for analytical and educational purposes and do not represent actual cases. The scenario-based method enables an assessment of how specific forensic workflows may assist investigators in corroborating allegations, preserving evidence integrity, reconstructing timelines, and ensuring procedural fairness.

Analytical Framework

The analysis is conducted through four interconnected dimensions:

[1] The Information Technology Act, 2000 (No. 21 of 2000), s 43A.
[2] Dhana Madhri Guruswamy, Treatise on POSH Act (Oakbridge Publications 2025).

1. **Legal Dimension** – Examination of statutory provisions, evidentiary requirements, and principles of natural justice applicable to POSH investigations.
2. **Technological Dimension** – Evaluation of digital forensic tools, workflows, and evidence preservation techniques.
3. **Governance Dimension** – Assessment of organisational responsibilities, Internal Committee preparedness, and compliance requirements.
4. **Ethical and Privacy Dimension** – Consideration of employee privacy rights, proportionality principles, confidentiality obligations, and data protection concerns.

Scope and Limitations

The study focuses primarily on workplace sexual harassment investigations conducted within Indian legal and regulatory frameworks. While reference is made to international forensic practices and technological developments, the analysis is confined to their relevance within the Indian POSH regime. The research does not involve primary empirical data collection through interviews, surveys, or case studies and therefore relies upon doctrinal and secondary-source analysis. The technological examples discussed are illustrative and may evolve with advancements in digital forensic science and emerging communication technologies.

Expected Contribution

The research seeks to contribute to the emerging scholarship at the intersection of employment law, digital forensics, and workplace governance by proposing a structured framework for the collection, preservation, analysis, and presentation of digital evidence in POSH proceedings. The study further aims to assist organisations, Internal Committees, legal practitioners, and policymakers in strengthening the integrity and effectiveness of workplace sexual harassment investigations in the digital age.

Literature Review

1. Workplace Sexual Harassment and the Evolution of POSH Jurisprudence

The legal discourse on workplace sexual harassment in India has evolved significantly since the landmark judgment of the Supreme Court in Vishaka v. State of Rajasthan (1997), which recognised sexual harassment as a violation of fundamental rights and laid down the Vishaka Guidelines.[3] Subsequent enactment of the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 ("POSH Act") institutionalised mechanisms for prevention and redressal through Internal Committees.[4]

Existing literature on workplace sexual harassment largely focuses on legal compliance, gender justice, organisational culture, reporting barriers, victimisation concerns, and the effectiveness of Internal Committees. Scholars such as Catharine MacKinnon have examined sexual harassment as a manifestation of gender-based power imbalance,[5] while Indian researchers have highlighted challenges relating to

[3] Vishaka v. State of Rajasthan, (1997) 6 SCC 241.

[5] Catharine A. MacKinnon, Sexual Harassment of Working Women: A Case of Sex Discrimination (Yale University Press 1979).

underreporting, confidentiality, procedural fairness, and inconsistent inquiry standards.

However, much of the existing scholarship continues to focus on traditional forms of workplace misconduct and interpersonal interactions, with limited examination of harassment occurring through digital communication platforms.

2. Digitalisation of Workplaces and Emerging Forms of Harassment

The rapid adoption of email systems, enterprise messaging platforms, social media, video conferencing applications, and cloud-based collaboration tools has transformed workplace communication. Researchers have increasingly observed that workplace harassment now frequently manifests through digital channels, including inappropriate emails, offensive messages, cyberstalking, non-consensual sharing of images, persistent online monitoring, and virtual meeting misconduct.

Studies examining cyber-harassment and online misconduct suggest that digital environments often create persistent and traceable records of behaviour. Unlike traditional verbal misconduct, digital communications generate metadata, timestamps, access logs, geolocation information, and communication histories that may serve as objective evidence during investigations.

While cyber-harassment literature has expanded substantially, the application of digital forensic methodologies specifically within workplace sexual harassment investigations remains relatively underexplored, particularly within the Indian legal framework.

3. Digital Forensics and Electronic Evidence

Digital forensics emerged as a specialised field focused on the identification, preservation, collection, analysis, and presentation of electronic evidence. Early scholarship by Casey (2011),[6] Nelson, Phillips and Steuart (2019),[7] and Carrier (2005)[8] established foundational principles relating to evidence integrity, forensic imaging, chain of custody, metadata analysis, and forensic reporting.

Contemporary research emphasises that digital forensic techniques have expanded beyond cybercrime investigations and are increasingly used in employment disputes, corporate misconduct inquiries, fraud investigations, and regulatory enforcement proceedings. Scholars have highlighted the significance of metadata analysis, email header examination, mobile device forensics, cloud forensics, multimedia authentication, and log analysis in reconstructing events and verifying factual claims.

Research further indicates that digital evidence often possesses greater reliability than testimonial evidence because it can independently corroborate timelines, user activities, communication patterns, and behavioural trends. Nevertheless, concerns remain regarding evidence manipulation, deepfake technologies, encrypted communications, and evolving cybersecurity threats.

4. Admissibility of Electronic Evidence and Indian Evidence Law

The legal treatment of electronic evidence has attracted significant scholarly attention in India. Following decisions such as Anvar P.V. v. P.K. Basheer (2014)[9] and Arjun Panditrao Khotkar v. Kailash Kushanrao

[6] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd edn, Academic Press 2011).

[7] Bill Nelson, Amelia Phillips and Christopher Steuart, Guide to Computer Forensics and Investigations (6th edn, Cengage Learning 2019).

[8] Brian Carrier, File System Forensic Analysis (Addison-Wesley 2005).

[9] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

Gorantyal (2020),[10] academic discourse has increasingly focused on authenticity, admissibility standards, certification requirements, and evidentiary reliability.

The enactment of the Bharatiya Sakshya Adhiniyam, 2023 has further reinforced the recognition of electronic records as a distinct category of evidence. Legal scholars have argued that courts and investigative bodies must develop greater technical understanding of digital evidence to ensure accurate evaluation of electronic records.[11]

Although significant literature exists regarding admissibility of electronic evidence in judicial proceedings, comparatively little attention has been paid to how Internal Committees under the POSH Act should evaluate and preserve electronic evidence during workplace investigations.

5. Privacy, Surveillance and Ethical Considerations

A parallel body of literature examines the tension between workplace investigations and employee privacy rights. Following the Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017), scholars have debated the permissible scope of workplace monitoring, employee surveillance, and access to personal devices.[12]

Research indicates that while digital forensic investigations can significantly improve fact-finding, excessive collection of personal information may create privacy risks, data protection concerns, and procedural fairness issues. International studies emphasise the importance of proportionality, necessity, informed consent, confidentiality safeguards, and minimisation principles during digital investigations.[13]

The literature therefore suggests a need to balance investigative effectiveness with privacy protection, particularly in sensitive workplace sexual harassment inquiries where personal communications and intimate information may become relevant.

Research Gap

The existing literature demonstrates extensive scholarship on workplace sexual harassment, electronic evidence, digital forensics, and privacy rights as independent fields of study. However, there remains limited interdisciplinary research examining how digital forensic techniques can be systematically integrated into workplace sexual harassment investigations under the POSH Act.

Specifically, there is a lack of structured guidance on:

- The role of digital forensic workflows in Internal Committee inquiries;
- Standards for collection and preservation of electronic evidence in POSH proceedings;
- Balancing digital evidence gathering with privacy and data protection obligations;
- Managing emerging challenges such as encrypted communications, cloud-based evidence, artificial intelligence, and deepfake technologies; and

[10] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[11] The Bharatiya Sakshya Adhiniyam, 2023 (No. 47 of 2023), ss 57 and 63.
[12] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[13] The Digital Personal Data Protection Act, 2023 (No. 22 of 2023), s 4.

- Developing organisational protocols for forensic readiness in workplace investigations.

This study seeks to address these gaps by proposing a structured digital forensic framework for workplace sexual harassment investigations and evaluating its legal, procedural, and practical implications within the Indian POSH regime.

Research Objectives

- To examine the legal significance of digital evidence in workplace sexual harassment investigations under the POSH Act.
- To analyse the applicability of digital forensic techniques in establishing facts and corroborating allegations.
- To identify legal, technological, and procedural challenges associated with the use of digital evidence in Internal Committee inquiries.
- To evaluate privacy, evidentiary, and natural justice concerns arising from forensic investigations.
- To propose a structured digital forensic framework for conducting fair, objective, and legally sustainable POSH investigations.

Investigating workplace sexual harassment through digital forensics

Sexual harassment investigations at workplace must be precise, sensitive and thorough tot find the facts ad truth,. Digital evidence such as emails, social media and other digital channels is common in today's workplaces. Digital forensics is essential for ensuring these investigations are accurate, ethical and legally valid.

Digital Forensics has three key components:

a. Foundations – foundations provide a framework for handling evidence.
b. Workflows – It describes techniques to extract and verify digital evidence.
c. Scenarios – it show how these techniques work in a real-world harassment cases.

Together these components form a comprehensive approach to solving complex workplace harassment allegations

Foundations of Digital Forensics

The foundations of digital forensics ensure investigations maintain integrity, credibility and admissibility in legal and internal proceedings. These pillars serve as backbone for structuring investigations and integrating workflows and scenarios. The three foundational pillars include:

Evidence Integrity and Chain of Custody

Maintaining the integrity of evidence and documenting its handling is vital to ensure the evidence is tamper-proof and admissible in court or internal proceedings.

Category	Details
Purpose	- To ensure the collected evidence remains authentic. Untampered and defensible in legal o internal proceedings
Key Workflows	- Hashing for Integrity Verification – Chain of Custody Documentation – Metadata Analysis

Involved	
Investigator's Actions	- Hashing Evidence – Generates has values for every piece of evidence at the tie of collection - Compares hash values during every stage of handling to confirm no alteration has occurred - Chain of Custody – Records every individual or entity who accesses the evidence during the investigation. Documents timestamps, access locations and reasons for handling the evidence - Metadata Preservation – Extracts and preserves metadata (e.g. timestamps, authorship, file creation) to prove evidence authenticity. Prevents metadata loss during copying or transfer of files
Scenarios where applied	- Emails: Hashing emails during collection and documenting every transfer between investigators and legal teams - CCTV Footage: ensuring that video files maintain the same hash before and after forensic analysis
Tools used	- FTK Imager : For evidence hashing and metadata preservation - Autopsy : For tracking evidence files and integrity checks - Magnet AXIOM – Comprehensive chain of custody tracking
Benefits	- Prevents evidence tampering allegations – Ensures evidence remains legally admissible. - Establishes investigator credibility in internal and legal proceedings

Digital Forensics Workflow

Digital forensics workflows describe the step-by-step methods used to handle and analyze evidence. These 16 workflows address all stages of evidence collection, authentication and reporting.

They include:

1. **Hashing**: Integrity verification of evidence
2. **Email Header Analysis** : Authenticating email origins and routing
3. **Geo-Location Tracking** – Verifying presence and movement
4. **Log Reviews** : Analyzing system and access logs for activity
5. **Metadata Analysis** : Authenticating digital files through embedded data
6. **Recovery of Deleted Data** : Restoring critical erased evidence
7. **Collaborative Tools Analysis** : Examining workplace tools for interactions
8. **Encrypted Data Recovery** : Unlocking protected files or communications
9. **Device Connectivity Logs** : Identifying proximity or device interactions
10. **Dark Web and Anonymous Activity**: Investigating hidden online actions
11. **Mobile Forensics**: Extracting app and communicating data from smartphones

12. **Audio and Video Authentication**: Verifying media legitimacy and detecting tampering
13. **Cloud Service Analysis**: Recovering shared or deleted files
14. **Browser History Analysis**: Establishing intent through web activity
15. **Wearable and IoT Device Analysis**: Extracting data from smart devices
16. **Psychological Profiling via Digital Behavior**: Analyzing tone and intent in communications

Each workflows serves as a specialized method for extracting and verifying evidence, ensuring investigators address all digital traces of harassment.

Dealing Workplace Harassment complaints through Digital Forensics

The table(s) explores real-world scenarios that investigators of workplace harassment complaints may encounter in workplace harassment cases. These scenarios demonstrate how workflows are applied in specific contexts.

Harassment via Emails and Shared Platforms

Category	**Details**
Scenario	The Complainant alleges receiving harassing emails from a manager and inappropriate comments in as hared Google Doc
Workflows Covered	Evidence Integrity Check, Email Header Analysis, Metadata Analysis, Collaborative Tools Analysis, Cloud Services Analysis, Timeframe Validation
Purpose	To establish a digital trail of harassment across email, shared documents, and collaborative tools while preserving integrity and admissibility
Investigator's Actions	- Collects emails and shared documents, exporting them in original formats (.eml, .msg. or .docx) to preserve metadata
	- Analyses email headers to trace the sender, verify IP addresses and detect spoofing
	- Examines metadata from the shared documents for timestamps, authorship, and modification history
	- Generates has values for all evidence at the time of collection to prevent tampering
	- Validates the consistency of timestamps between emails, shared documents and the complainant's timeline
Findings	- Emails contained harassing content corroborated by metadata linking them to the accused's account
	- Shared document metadata confirmed inappropriate edits and matched the complainant's claims
	- All evidence was preserved with validated hash values for legal admissibility

Harassment via Social Media and Messaging Platforms

Category	Details
Scenario	The Complainant alleges receiving messages on LinkedIn, WhatsApp or other messaging platforms
Workflows Covered	Social Media Analysis, Mobile Forensics, Metadata Analysis, Chain of Custody Documentation, Browser History Analysis
Purpose	To validate harassment allegations by analyzing inappropriate messages on social media and messaging platforms while ensuring evidence authenticity
Investigator's Actions	- Extracts messages from LinkedIn and WhatsApp using forensic tools, preserving metadata (e.g. timestamps, sender details)
	- Cross references message timestamps with other evidence, such as email or shared file logs
	- Analyses browser history for signs of stalking behavior, such as repeated visits to the complainants' profiles
	- Hashes all extracted evidence to maintain integrity and ensure admissibility in legal proceedings
Findings	- Metadata validated inappropriate messages originated from the accused's accounts
	- Browser history revealed stalking behavior aligned with the complainants' claims
	- Evidence was preserved and cross-referenced for timeline consistence

Harassment in Physical and Workplace Environments

Category	Details
Scenario	The Complainant alleges verbal harassment in a shared workspace, corroborated by CCTV footage and IoT logs
Workflows Covered	Device Connectivity Logs, Geo-Location Tracking, Audio and Video Authentication, Metadata Analysis, IoT Device Analysis, Timeframe Validation
Purpose	To corroborate harassment claims using physical evidence, such as CCTV footage and wearable logs and IoT logs
Investigator's Actions	- Secures raw CCTV footage and wearable logs, analyzing timestamps and proximity details
	- Verifies metadata from IoT logs (e.g. smart door entries) to confirm the accused's presence during the alleged incident
	- Uses forensic tools to authenticate the CCTV footage and confirm its consistency with other evidence

	- Correlated all data sources to validate the complaints' timeline and claims
Findings	- CCTV logs confirmed the accused's presence and matched the complainant's timeline
	- Wearable data validated the complainant's emotional distress during the incident
	- All evidence was authenticated and preserved for admissibility

Data Tampering and Retaliation by the Accused

Category	**Details**
Scenario	The Complainant alleges the accused deleted inappropriate files or tampered with shared documents in retaliation
Workflows Covered	Recovery of Deleted Data, Metadata Analysis, Cross-Platform Synchronization, Log Reviews, Sentiment Analysis
Purpose	To uncover evidence of tampering, deletion, or retaliation by analyzing recovered data and log activities
Investigator's Actions	- Uses recovery tools to restore deleted emails, messages or shared files
	- Analyses metadata for recovered files to determine creation, modification and deletion timestamps
	- Reviews synchronization logs to trace when files were uploaded, edited or deleted
	- Conducts sentiment analysis on workplace communications to detect retaliatory tone or behavior
Finding	- Deleted files were successfully recovered, revealing tampered content
	- Metadata confirmed intentional deletions and unauthorized edits linked to the accused
	- Sentiment analysis identified a pattern of retaliation in communication

Cyberstalking and Unauthorized Monitoring

Category	**Details**
Scenario	The Complainant alleges unauthorized tracking of their location or activities using GPS, IoT devices or spyware
Workflows Covered	Geo-Location Tracking, Metadata Analysis, IoT Device Analysis, Dark Web and Anonymous Activity, Log Reviews
Purpose	To confirm unauthorized tracking or monitoring by analyzing geolocation logs, IoT activity, or malicious software

Investigator's Actions	- Analyses GPS logs from the complainant's and accused's devices to identify tracking patterns and timestamps
	- Reviews IoT device logs (e.g. smart cameras or trackers) to detect unauthorized access by the accused
	- Investigates dark web or anonymous platforms for links to spyware or monitoring tools tied to the accused
	- Corelates geolocation data with other evidence such as emails or messages to establish intent and notice
Findings	- GPS confirmed the accused tracked the complainant without authorization
	- Metadata linked spyware of the accused's device or account, corroborating claims of unauthorized monitoring
	- Evidence showed consistent tracking aligned with the complainant's allegations

Persistent Harassment Across Platforms

Category	**Details**
Scenario	The Complainant alleges repeated harassment across multiple platforms, including emails, messaging apps and workplace tools
Workflows Covered	Cross-Platform Synchronization, Collaborative Tools Analysis, Social Media Analysis, Chain of Custody Documentation
Purpose	To prove persistent harassment by linking data from multiple platforms and creating a consistent timeline of incidents
Investigator's Actions	- Merges and analyzes data from different platforms, such as emails, Slack, WhatsApp and LinkedIn, to identify harassment patterns
	- Extracts synchronization logs to trace the flow of messages, files or inappropriate comments across platforms
	- Documents all evidence in a chain of custody to ensure its integrity and admissibility in legal proceedings
	- Corelates harassment incidents with timestamps and other evidence to establish a consistent narrative
Findings	- Harassment was confirmed across Slack, WhatsApp and email platforms with consistent patterns established
	- Synchronizations logs revealed inappropriate messages and shared files originated from the accused
	- Chain of custody ensured all evidence remained unaltered and legally admissible

Multimedia Evidence Authentication

Category	Details
Scenario	A video or audio recording (e.g. Zoom meeting) is submitted as evidence of harassment, with claims of tampering by the opposing party
Workflows Covered	Audio and video Authentication, Metadata Analysis, Hashing, Chai of Custody Documentations
Purpose	To ensure the multimedia evidence remains untampered and admissible in court while verifying its authenticity
Investigator's Actions	- Secures raw recording flies (e.g. .mp4, .avi) from original sources without compression or conversion to preserve metadata
	- Examines metadata (e.g. timestamps, file size and authorship) to confirm authenticity and detect tampering
	- Uses hashing tools to generate a hash value for the file at collection and verifies the has after any forensic analysis
	- Enhances audio or video (if necessary) for better clarity while ensuring the original file remain unaltered
Findings	- Multimedia evidence was verified as authentic, with no signs of tampering or deepfake manipulation
	- Metadata aligned with he complainant's timeline, confirming the recording's relevance
	- Hashing ensured evidence integrity throughout the investigation process

Digital forensics aids workplace sexual harassment investigations using structured processes and methods. These provide technical support and practical examples based on principles like preserving evidence, analyzing metadata and creating timelines. This framework makes investigations reliable and empowers investigators to find truth, confirm claims and ensure justice.

Conclusion and recommendation statement

The increasing digitisation of workplaces has fundamentally altered both the nature of workplace sexual harassment and the methods available for its investigation. As professional interactions migrate to digital platforms, electronic evidence has become indispensable in establishing factual narratives and reducing dependence on conflicting oral testimonies. Digital forensics therefore represents a significant advancement in ensuring objectivity, transparency and fairness in investigations conducted under the POSH Act.

However, the integration of digital forensic techniques into Internal Committee proceedings also raises important legal and ethical concerns relating to privacy, proportionality, data protection, evidentiary integrity and procedural fairness. Internal Committees must therefore adopt scientifically validated evidence collection procedures while ensuring compliance with statutory safeguards and principles of

natural justice.

The study suggests that organisations should formulate comprehensive digital evidence preservation policies, establish standard operating procedures for forensic collection, provide specialised training to Internal Committee members, and engage certified forensic experts wherever necessary. The Ministry of Women and Child Development and regulatory authorities may also consider issuing detailed guidelines for handling electronic evidence in POSH proceedings to promote consistency and legal certainty across organisations.[14][15]

As artificial intelligence, encrypted communications, cloud computing and deepfake technologies continue to evolve, workplace investigations will increasingly require multidisciplinary expertise combining law, technology and forensic science. The future effectiveness of the POSH framework will therefore depend not merely upon legal compliance but upon the responsible integration of digital forensic capabilities that protect both the dignity of complainants and the procedural rights of respondents. Strengthening forensic preparedness will ultimately contribute towards safer, more transparent and more accountable workplaces in the digital era.

References

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). Academic Press.

Guruswamy, D. M. (2025). *Treatise on POSH Act*. Oakbridge Publications.

Kaushik, A. (2024). *Guide to prevention of sexual harassment at workplace*. Law Publishing House.

MacKinnon, C. A. (1979). *Sexual harassment of working women: A case of sex discrimination*. Yale University Press.

Nain, B. (2023). *FAQs on the POSH Act*. Bharat Law House.

Nelson, B., Phillips, A., & Steuart, C. (2019). *Guide to computer forensics and investigations* (6th ed.). Cengage Learning.

Rai, R. (2022). *P.O.S.H.: A complete reference book on prevention of sexual harassment of women at workplace for students and professionals*. Sankalp Publication.

[14] Indian Institute for Human Settlements, Safe Workplaces for All: A Trainer's Guide for Internal Committees under the POSH Act (IIHS 2022) <https://iihs.co.in/knowledge-gateway/safe-workplaces-for-all-a-trainers-guide-for-internal-committees-under-posh-act/> accessed 20 July 2026.

[15] Anil Kaushik, Guide to Prevention of Sexual Harassment at Workplace (Law Publishing House 2024).

A. Statutes and Legislation

- The Bharatiya Sakshya Adhiniyam, 2023 (No. 47 of 2023).
- The Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
- The Information Technology Act, 2000 (No. 21 of 2000).
- The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (No. 14 of 2013).

B. Cases

- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Vishaka v. State of Rajasthan, (1997) 6 SCC 241.

C. Reports, Guidelines and Online Sources

- Indian Institute for Human Settlements, Safe Workplaces for All: A Trainer's Guide for Internal Committees under the POSH Act (IIHS 2022) <https://iihs.co.in/knowledge-gateway/safe-workplaces-for-all-a-trainers-guide-for-internal-committees-under-posh-act/> accessed 20 July 2026.
- Ministry of Women and Child Development, Handbook on Sexual Harassment of Women at Workplace (Government of India 2015).
- Indian Kanoon <https://indiankanoon.org> accessed 20 July 2026.
- Manupatra <https://www.manupatrafast.com> accessed 20 July 2026.
- SCC Online <https://www.scconline.co