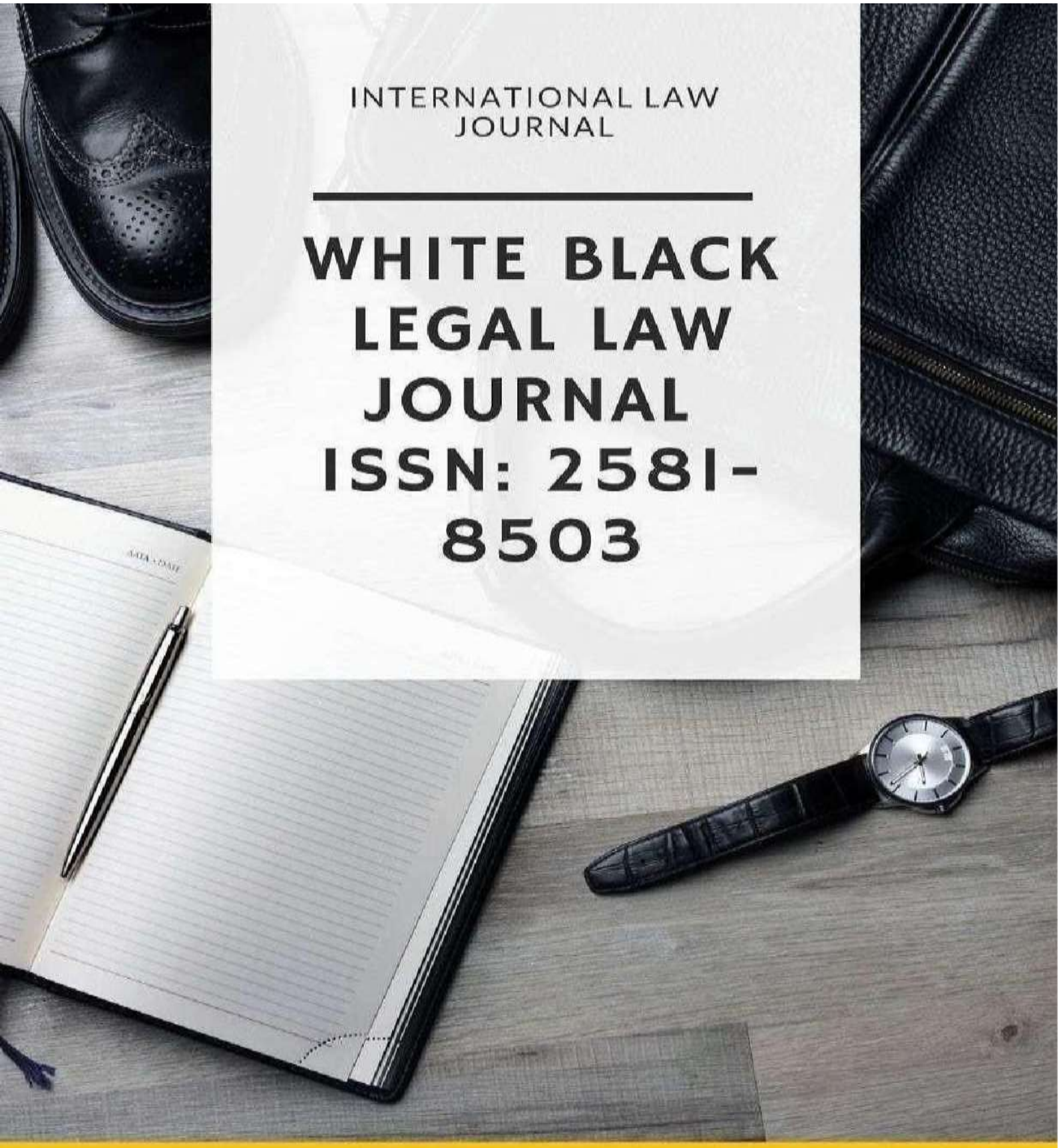

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | June 2025 ISSN: 2581-8503

DIGITAL SEXUAL HARASSMENT IN INDIA: EVALUATING LEGAL FRAMEWORKS AND ENFORCEMENT CHALLENGES

AUTHORED BY - ANUSHTHA SONI

Abstract

The rapid proliferation of digital technologies and internet penetration in India has revolutionised communication but has also facilitated new forms of gender-based violence, particularly digital sexual harassment. From cyberstalking and non-consensual image sharing to sexually explicit trolling and deep fake pornography, the digital space has become a perilous environment, especially for women and marginalised genders. While India has enacted laws under the Information Technology Act, 2000 and the Indian Penal Code, 1860 to address such offences, significant gaps remain in terms of definition, implementation, jurisdiction, and victim protection. This research paper critically examines the legal frameworks addressing digital sexual harassment in India and evaluates their effectiveness through an analysis of recent cases, enforcement mechanisms, and institutional responses. It also explores the challenges victims face in accessing justice, including patriarchal biases, procedural delays, lack of digital literacy, and limited cyber infrastructure. The paper concludes by suggesting reforms to strengthen legal safeguards, improve enforcement, and ensure a more victim-centric approach to justice in the digital age.

Keywords

Digital sexual harassment; cybercrime; Indian legal system; Information Technology Act, 2000; Indian Penal Code, 1860; online gender-based violence; cyberstalking; non-consensual pornography; legal enforcement; victim protection; digital rights; cyber law reform.

Literature Review

The phenomenon of digital sexual harassment has gained increasing scholarly attention with the expansion of cyberspace and the unique challenges it poses to traditional legal systems. Scholars such as NVidia Menon and Ratna Kapur have examined how digital spaces replicate patriarchal control and exacerbate gendered vulnerabilities. Their work suggests that the

internet, while often hailed as a liberating force, can become a site for the extension of societal misogyny.

Legal literature reveals a growing critique of the Information Technology Act, 2000, particularly sections 66E, 67, and 67A, for their limited scope and vague definitions. Studies by legal experts like Apar Gupta and Pranesh Prakash have highlighted how enforcement agencies often misuse these provisions or fail to apply them altogether due to a lack of training and awareness. Furthermore, the Indian Penal Code provisions, including Sections 354A (sexual harassment) and 509 (insulting the modesty of a woman), are frequently invoked without addressing the digital nuances of harassment.

Empirical research, such as that conducted by the Internet Democracy Project and Amnesty International, underscores the psychological and social toll digital sexual harassment has on victims, often leading to self-censorship, mental trauma, and withdrawal from online spaces. These reports also critique the inefficiencies in India's complaint mechanisms and the lack of timely redressal from law enforcement agencies.

Feminist scholars have also stressed the importance of intersectionality in understanding digital harassment. Marginalised groups—particularly Dalit women, LGBTQ+ individuals, and religious minorities—often experience compounded harassment online. This intersectional gap is rarely addressed in mainstream policy or legal discourse.

In addition, international perspectives provide valuable comparative insights. The legislative models in countries like the UK, Canada, and Australia offer more precise definitions of cyber-harassment and better victim protection frameworks, prompting Indian scholars to advocate for similar reforms in the domestic context.

Despite the availability of fragmented academic and legal analyses, there remains a significant gap in comprehensive, interdisciplinary research focused on the enforcement challenges and victim-centric legal reform in India. This research paper seeks to fill that gap by synthesizing legal critique, case law analysis, and policy recommendations.

Research Methodology

This research adopts a **doctrinal and qualitative approach**, focusing on the critical analysis of statutory provisions, judicial pronouncements, secondary literature, and policy documents related to digital sexual harassment in India. The study primarily relies on **primary legal sources** such as the **Information Technology Act, 2000**, the **Indian Penal Code, 1860**, and relevant **Supreme Court and High Court judgments** to understand the legal framework addressing digital sexual offences.

To evaluate the **implementation and enforcement challenges**, the study also draws upon **secondary sources**, including law review articles, empirical studies by NGOs and digital rights organisations, government reports, and expert commentaries. These materials provide insight into the practical difficulties faced by victims in accessing justice and the institutional barriers that hinder effective enforcement.

The methodology includes:

- **Statutory Analysis**: Examining the scope, language, and applicability of relevant legal provisions.
- **Case Law Review**: Studying landmark and recent judicial decisions that interpret or apply laws related to digital sexual harassment.
- **Comparative Analysis**: Evaluating international legal frameworks to understand best practices that could be adapted to the Indian context.
- **Thematic Content Analysis**: Reviewing academic literature and reports to identify recurring issues and proposed reforms.

The research is **descriptive, analytical, and exploratory** in nature. It aims not only to assess the adequacy of existing laws but also to identify **systemic shortcomings** and recommend **policy-level interventions** that are both legally sound and socially sensitive.

Hypothesis

This study is premised on the hypothesis that the existing legal frameworks addressing digital sexual harassment in India are insufficient to effectively deter and redress such offenses. It is posited that:

1. **Inadequate Legal Definitions and Provisions:**

The statutory provisions under the Information Technology Act, 2000 and the Indian Penal Code, 1860 do not adequately capture the nuances of digital sexual harassment, resulting in ambiguous interpretations and inconsistent applications in judicial proceedings.

2. **Enforcement and Institutional Challenges:**
   The current enforcement mechanisms suffer from systemic challenges, including insufficient training of law enforcement personnel in digital crimes, procedural delays, and limited resources. These challenges contribute to a significant gap between legal intent and practical redress for victims.
3. **Need for Victim-Centric Reform:**
   A lack of comprehensive victim support systems and the prevailing patriarchal socio-cultural context further compound the difficulties faced by survivors in accessing justice. Reforms that incorporate victim-centric approaches and updated technological insights are hypothesized to be essential for more effective deterrence and remediation.

Each of these hypotheses will be examined through doctrinal analysis, case law reviews, and comparative studies with international best practices, forming the basis for the critical evaluation of legal frameworks and enforcement challenges discussed in the subsequent sections of the paper.

Introduction

The digital revolution in India, marked by widespread internet access and the proliferation of smartphones, has redefined social interaction, communication, and the dissemination of information. However, alongside these advancements has emerged a disturbing trend: the increase in digital sexual harassment. Acts such as cyberstalking, online sexual bullying, unsolicited sharing of explicit content, and deep fake pornography have created new dimensions of abuse that were previously unimaginable in traditional settings[1]. The anonymity and reach provided by the internet embolden perpetrators while leaving victims exposed to a continuous cycle of trauma, often without adequate recourse.

While India has responded to these threats with legislative instruments like the **Information Technology Act, 2000** and selective amendments to the **Indian Penal Code, 1860**, these measures are often reactive rather than preventative. For instance, Section 66E of the IT Act

[1]Ayesha Khan, 'Digital Violence Against Women in India' (2020) 15(2) *Journal of Cyber Law and Policy* 23.

criminalises the violation of privacy, and Sections 67 and 67A address the publication and transmission of obscene and sexually explicit material. Simultaneously, provisions such as Sections 354A and 509 of the IPC are employed to tackle sexual harassment in broader contexts[2]. Yet, the convergence of these laws often leads to jurisdictional overlaps, enforcement delays, and interpretational inconsistencies that undermine the effectiveness of redressal mechanisms.

The growing digital presence of women and LGBTQ+ individuals has made them especially vulnerable to gender-based violence online. Several national and international studies report that women in India routinely face harassment ranging from rape threats and sexual slurs to the misuse of personal images on social media platforms[3]. In many cases, law enforcement agencies lack the technological competence or gender sensitivity to respond appropriately, resulting in victims withdrawing from online spaces or not reporting incidents at all.

This research seeks to critically evaluate the Indian legal framework governing digital sexual harassment and to identify the structural and procedural challenges in its enforcement. By examining statutory provisions, judicial interpretations, and enforcement practices, the paper aims to assess whether the existing legal system provides adequate protection and justice to victims. The study also highlights the necessity for reform by comparing Indian laws with international legal models and suggesting victim-centric policy measures.

The issue is not merely legal but deeply socio-cultural, requiring a shift in both jurisprudence and enforcement ideology. In the absence of robust legal protections and effective enforcement, the digital realm risks becoming an unsafe space for marginalised voices, thereby threatening democratic participation, free expression, and individual dignity.

1. Understanding Digital Sexual Harassment: Forms and Manifestations

Digital sexual harassment refers to the use of technology—particularly the internet, social media, and mobile communication—to perpetrate sexual abuse, harassment, or intimidation. Unlike traditional forms of sexual harassment, digital harassment is marked by its **pervasive reach, anonymity, permanence, and replicability**, making it a uniquely harmful form of

[2]Usha Ramanathan, 'Technology and the Law: Limits of Legal Reform in Addressing Online Harassment' (2018) *Indian Journal of Law and Technology* 31.
[3]Amnesty International, 'Troll Patrol India: Exposing Online Abuse Faced by Women Politicians' (2020)

abuse in the modern era. Victims are often left with profound psychological trauma, reputational damage, and limited avenues for legal redress due to the evolving nature of technology and inadequate enforcement mechanisms[4].

1.1 Common Forms of Digital Sexual Harassment

Several patterns of digital sexual harassment have emerged in India in recent years, including but not limited to:

- **Cyberstalking**: Persistent and unwanted digital surveillance and communication intended to threaten or intimidate the victim.
- **Non-consensual image sharing** (revenge porn): The distribution of private, intimate images without the subject's consent, often with malicious intent[5].
- **Sexually explicit trolling and threats**: Sending abusive, sexual, or threatening messages on public or private forums.
- **Deepfake pornography**: Using artificial intelligence to create fabricated sexual content that falsely depicts individuals in explicit acts[6].
- **Online doxxing**: Publishing private information like addresses or phone numbers online to invite harassment or real-world harm.

1.2 Victim Demographics and Patterns

Research suggests that women, transgender persons, and other gender and sexual minorities are disproportionately targeted by digital sexual abuse. The nature of attacks often reflects deep-rooted caste, class, and communal biases. For instance, Dalit and Adivasi women often face casteist slurs in conjunction with sexual abuse online, a phenomenon that mainstream legal definitions largely overlook[7].

Further, young adults and adolescents are increasingly becoming targets due to their high presence on social media. Cases of "sextortion" and online grooming have also been reported, wherein perpetrators exploit minors for sexual favours using threats of digital exposure[8].

[4]Vrinda Bhandari and Renuka Sane, 'An Analysis of the Regulatory Framework for Digital Harassment in India' (2021) *Centre for Internet and Society*
[5]NandiniChami and Anita Gurumurthy, 'Surveillance, Gender, and the Rights-Based Approach to Privacy' (2019) *IT for Change* 12.
[6]DeepaSeetharaman and Jeff Horwitz, 'Fake Porn Videos Are Being Weaponized to Harass and Humiliate Women' *Wall Street Journal* (13 February 2019).
[7]ThenmozhiSoundararajan, 'Digital Caste Violence: The New Face of Online Discrimination in India' (2022) *Equality Labs Report*.
[8]Childline India Foundation, 'Online Child Sexual Exploitation in India' (2020)

Despite the growing prevalence of these incidents, societal stigma often deters victims from reporting them, resulting in a gross underestimation of the problem.

1.3 Challenges of Definition and Legal Recognition

A significant problem in addressing digital sexual harassment is the **lack of comprehensive legal definitions**. Indian law tends to treat online offences as extensions of offline sexual crimes without accounting for their unique characteristics. This creates ambiguity in judicial interpretation and procedural handling. For example, while Section 354A of the IPC criminalises sexual harassment, it does not explicitly cover non-consensual distribution of images unless they are deemed obscene, leaving many victims without recourse.

Moreover, the binary treatment of public versus private spaces under Indian law fails to account for the hybrid nature of digital environments—where private messages can go viral instantly and where harm can occur in spaces that are simultaneously public and intimate.

2. Legal Framework Governing Digital Sexual Harassment in India

India's legal response to digital sexual harassment is built upon a **combination of general criminal law and specific cyber law provisions**, primarily through the **Indian Penal Code, 1860 (IPC)** and the **Information Technology Act, 2000 (IT Act)**. While these legislations provide a legal foundation for prosecuting cyber-based sexual offences, they are **fragmented, reactive, and often inadequate** in addressing the evolving nature of digital crimes.

2.1 Indian Penal Code Provisions

The IPC was originally crafted in a pre-digital era but has been amended to accommodate some technology-related offences. Relevant sections include:

- **Section 354A**: Defines and penalises sexual harassment, including unwelcome sexually coloured remarks and demands for sexual favours. It is often invoked in cases of online trolling and unsolicited messages.
- **Section 354D**: Criminalises stalking, including cyberstalking.
- **Section 509**: Punishes any act intended to insult the modesty of a woman, such as sending obscene or derogatory messages via electronic communication[9].

[9]Indian Penal Code 1860, ss 354A, 354D, 509.

Although these sections are valuable in establishing the **intention and impact** of harassment, they are often **limited by their gendered language**, applying primarily to women and thereby excluding other vulnerable groups such as LGBTQ+ individuals[10].

2.2 Information Technology Act, 2000

The IT Act serves as India's principal legislation dealing with cyber offences. Key provisions include:

- **Section 66E**: Punishes the capture, publication, or transmission of images of private areas without consent.
- **Section 67**: Criminalises the publishing or transmission of obscene material in electronic form.
- **Section 67A**: Pertains specifically to sexually explicit content and carries more severe penalties.
- **Section 72**: Penalises the breach of confidentiality and privacy by anyone who, in pursuance of any power under the Act, accesses personal data without the owner's consent[11].

However, these sections have been **criticised for vague language** and inconsistent interpretation by law enforcement. Moreover, the burden of proof often falls heavily on the victim, particularly when obscenity is judged by subjective community standards[12].

2.3 Judicial Interventions and Gaps

Indian courts have attempted to interpret these provisions progressively. In *Shreya Singhal v Union of India*, the Supreme Court struck down Section 66A of the IT Act for being vague and violative of free speech[5]. Although the judgment was seen as a victory for digital rights, it left a vacuum in regulating offensive online speech, including harassment.

Further, courts have repeatedly urged law enforcement agencies to be proactive in handling complaints of online abuse. Yet, in many instances, **First Information Reports (FIRs) are not registered promptly**, and victims are subjected to humiliating questions that deter them from pursuing justice.

---

[10]Vrinda Grover, 'Gender, Technology, and Law: Beyond Binary Legal Protections' (2021) *Law and Society Review* 112.
[11]Information Technology Act 2000, ss 66E, 67, 67A, 72.
[12]Pavan Duggal, 'Cyber Law in India: The Emerging Trends' (2020) *Cyber Law Journal* 14.

Judicial recognition of digital harassment is growing, but remains hindered by **lack of consistent jurisprudence** and **the absence of a comprehensive cybercrime code**. Additionally, offences under the IPC and IT Act are often charged separately, resulting in procedural confusion and delays in prosecution.

3. Enforcement Challenges and Institutional Barriers

Despite the existence of statutory provisions addressing digital sexual harassment, **implementation remains a significant challenge** in India. Victims often face procedural roadblocks, technological illiteracy among enforcement officials, social stigma, and a lack of institutional sensitivity. These barriers contribute to the **under-reporting, poor investigation, and delayed prosecution** of digital sexual offences.

3.1 Inadequate Police Infrastructure and Training

One of the most pressing issues is the **lack of digital forensics training and cybercrime investigation capacity** within police forces. Many law enforcement officers are either unaware of relevant provisions under the IT Act and IPC or are reluctant to file First Information Reports (FIRs) unless the harm is severe or tangible[13]. Furthermore, victims often report that police responses are dismissive, especially when the abuse occurs on social media or messaging platforms.

The establishment of **cybercrime cells** in metropolitan areas was intended to address these shortcomings, yet their reach remains limited. In rural and semi-urban areas, access to trained personnel and technological resources is even scarcer.

3.2 Victim Reluctance and Social Stigma

Digital sexual harassment is often viewed through a **moralistic lens**, where victims—especially women—are blamed for their online presence or accused of inviting attention. Such victim-blaming attitudes dissuade many from reporting abuse, fearing reputational harm, family backlash, or even job loss[14].

[13]Rina Mukherji, 'Cyber Crime Policing in India: Still a Distant Dream' (2022) *Economic and Political Weekly* Vol 57(12) 34
[14]Aditi Bhatia, 'Shaming the Victim: A Study of Social Media Harassment in Urban India' (2021) *Feminist Media Studies* 19(2) 187

For LGBTQ+ individuals, Dalit women, and other marginalised groups, reporting such crimes may further expose them to **institutional bias and discrimination**. The absence of anonymity in legal processes exacerbates the trauma, leaving many victims without safe recourse[4].

3.3 Jurisdictional and Procedural Confusion

Digital crimes often transcend **geographic and legal boundaries**, creating jurisdictional confusion. A perpetrator located in one state or country may harass a victim in another, complicating the process of investigation and arrest. This transboundary nature of digital sexual harassment **demands inter-agency coordination**, which is often lacking due to bureaucratic inertia and poor technological infrastructure[15].

Moreover, the Indian legal system is not well-equipped to handle the **speed required for digital evidence collection**. Delays in seizing devices, extracting metadata, or contacting social media companies for user data can result in loss or manipulation of critical evidence.

3.4 Weak Institutional Redress Mechanisms

Although platforms like the **National Cyber Crime Reporting Portal** (cybercrime.gov.in) have been launched to streamline complaint mechanisms, victims frequently report unresponsiveness and delays. The portal lacks follow-up infrastructure, and most complaints are redirected to local police stations, where the earlier mentioned limitations persist[16].

Additionally, there is no **specialised tribunal or fast-track court** to deal with cyber sexual offences. The overburdened judiciary leads to prolonged trials, which are emotionally exhausting and legally complex for victims seeking justice.

4. Comparative Legal Analysis: Global Best Practices

In assessing India's legal and enforcement framework against digital sexual harassment, it is instructive to examine **international approaches** that offer more comprehensive protections, victim support mechanisms, and enforcement models. Comparative analysis can help identify reforms suitable for India's socio-legal context.

[15]Pratik Sinha, 'Digital Jurisdiction and Law Enforcement: Challenges in the Indian Context' (2021) *Cyber Law Bulletin* 8(3) 66
[16]National Cyber Crime Reporting Portal, Ministry of Home Affairs, Government of India

4.1 The United Kingdom

The UK's **Sexual Offences Act 2003**, supplemented by the **Malicious Communications Act 1988** and the **Communications Act 2003**, provides robust mechanisms for tackling online sexual harassment. The UK explicitly criminalises sending offensive or threatening messages online, with specific emphasis on **harm caused by digital communications**[17].

Further, the UK has established the **Online Harms White Paper**, a policy framework aiming to hold digital platforms accountable for preventing and removing harmful content, including sexual harassment. This model balances **free speech** with protections for vulnerable users, backed by specialized cybercrime units and victim support services.

4.2 Australia

Australia's **Criminal Code Act 1995** incorporates offences like **cyberstalking, image-based abuse**, and **revenge porn** with clear definitions and strong penalties[18]. The **Enhancing Online Safety Act 2015** establishes the Office of the eSafety Commissioner, which provides victims with a direct reporting mechanism, educates the public, and enforces take-down orders against harmful content.

Australia's victim-centric approach includes **fast-tracking complaints** and promoting digital literacy, alongside law enforcement training to handle cyber offences sensitively and efficiently.

4.3 European Union

The **General Data Protection Regulation (GDPR)**, combined with the **Directive on Combating Violence Against Women**, offers a multi-layered approach integrating privacy rights, data protection, and gender-based violence legislation[19]. The EU mandates member states to adopt victim-centric policies and enhance coordination between agencies, emphasizing **preventive and educational strategies**.

The EU's approach also incorporates platform accountability, requiring social media and

[17]Sexual Offences Act 2003 (UK); Communications Act 2003 (UK).
[18]Criminal Code Act 1995 (Cth) ss 474.17, 474.19.
[19]Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime (Victims' Rights Directive).

online intermediaries to implement proactive measures against digital sexual harassment, including content moderation and swift response systems.

4.4 Lessons for India

India's legal framework can benefit from these global best practices by:

- **Establishing specialized cybercrime units** with adequate training and resources.
- **Creating victim support mechanisms** that ensure confidentiality, psychological counselling, and legal aid.
- **Mandating platform responsibility** to prevent and remove digital sexual harassment promptly.
- **Enacting comprehensive legislation** that clearly defines digital sexual harassment and addresses emerging technological challenges.

Integrating these elements could strengthen India's capacity to protect victims while upholding digital freedoms.

5. Recommendations and Policy Reforms

Addressing digital sexual harassment in India requires a **multi-pronged approach** involving legislative amendments, institutional capacity building, victim support, and public awareness campaigns. This section outlines key recommendations based on the gaps identified in existing laws and enforcement practices, drawing from both domestic challenges and international best practices.

5.1 Legislative Reforms

India's laws should be **updated and consolidated** to explicitly recognize digital sexual harassment in its many forms. This includes:

- Introducing a **comprehensive legal definition** of digital sexual harassment that covers non-consensual image sharing, cyberstalking, deepfakepornography, and online threats.
- Amending the IPC and IT Act to provide **gender-neutral protections**, ensuring that all victims, including transgender and non-binary individuals, are covered[20].

[20]Vrinda Grover, 'Inclusive Legal Protections for Gender and Sexual Minorities' (2021) *Human Rights Law Review* 24(1) 67

- Enacting provisions that impose **clear obligations on digital platforms** to monitor, report, and remove harmful content within stipulated timelines.

5.2 Strengthening Enforcement Mechanisms

- Establish **specialised cybercrime units** across all states, equipped with forensic expertise and technological infrastructure to handle complex digital evidence[21].
- Provide **training and sensitisation programs** for law enforcement, judiciary, and prosecutors to understand the nuances of digital sexual harassment and victim trauma.
- Develop **fast-track courts** or tribunals specifically for cyber offences to ensure timely justice and reduce backlog.

5.3 Victim-Centric Support Systems

- Create **confidential reporting mechanisms** that protect victims' privacy and reduce the fear of social stigma[22].
- Institutionalise access to **counselling, legal aid, and rehabilitation** services for victims of digital sexual harassment.
- Promote **digital literacy programs** to empower users about their rights, privacy settings, and reporting avenues.

5.4 Public Awareness and Education

- Launch nationwide **awareness campaigns** targeting schools, colleges, workplaces, and rural areas to educate people about digital sexual harassment and its consequences.
- Engage **community leaders, NGOs, and media** to challenge victim-blaming attitudes and promote respectful online behaviour.

5.5 Enhancing Platform Accountability

- Implement **regulatory frameworks** that mandate social media companies and internet service providers to develop robust content moderation policies.
- Encourage platforms to **collaborate with law enforcement** and civil society for swift identification and removal of abusive content.

---

[21]Rina Mukherji, 'Cybercrime Policing in India: Capacity Building and Challenges' (2022) *Economic and Political Weekly* 57(12) 38

[22]Childline India Foundation, 'Ensuring Confidentiality in Cyber Harassment Reporting' (2020)

- Explore **technological solutions** such as AI-based monitoring while ensuring these do not infringe on free speech and privacy rights.

Conclusion

Digital sexual harassment in India represents a growing challenge that intersects technology, gender, and law enforcement. Despite the presence of various legal provisions under the Indian Penal Code and the Information Technology Act, these laws remain **fragmented and insufficiently responsive** to the complex and evolving nature of online abuse. Enforcement mechanisms are hindered by lack of training, institutional inertia, social stigma, and procedural inefficiencies, which collectively deter victims from reporting and seeking justice.

The comparative analysis with countries such as the United Kingdom, Australia, and members of the European Union highlights the need for **comprehensive, victim-centric legislation** supported by well-equipped enforcement agencies and robust platform accountability frameworks. India must reform its legal architecture to adopt **clear definitions, gender-neutral protections, and faster adjudication processes**. Additionally, investing in digital literacy and public awareness is critical to transforming societal attitudes that perpetuate victim-blaming and silence survivors.

The **path forward** requires a holistic approach that balances protection of victims, respect for fundamental rights, and the challenges posed by rapidly advancing digital technologies. Only through coordinated legislative reform, institutional strengthening, and social sensitisation can India effectively confront and reduce the menace of digital sexual harassment, ensuring a safer and more equitable digital space for all its citizens.