JAAFR INTERNATIONAL RESEARCH JOURNAL
JOURNAL OF ADVANCE AND FUTURE RESEARCH
JAAFR.ORG | ISSN : 2984-889X
An International Open Access, Peer-reviewed, Refereed Journal

ONLINE HARASSMENT: LEGAL PROTECTION FOR WOMEN AND CHILDERN

[1] M. Mohammed Arshad Khan,[2] Amutha Lakshmi
[1]Student,[2]Assistant Professor
[1]SCHOOL OF LAW,
[1]VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCE STUDIES, CHENNAI, INDIA.

Abstract: India's rapid digital expansion, with over 900 million internet users by 2024, has enabled unprecedented connectivity while simultaneously fuelling a sharp escalation in online harassment disproportionately targeting women and children. Cyberstalking, non-consensual intimate image sharing, doxxing, sexual threats, impersonation, and child grooming have emerged as defining harms of the digital age, rooted in pre-existing structural inequalities now amplified by technology.

This study undertakes a comprehensive doctrinal examination of India's legal framework governing online harassment of women and children, evaluating its constitutional foundations, statutory architecture, regulatory mechanisms, and judicial doctrines. The constitutional framework under Articles 14, 15, 19, and 21 is analysed as the normative standard against which all legislative responses are assessed, drawing on landmark judgments including *Puttaswamy* (privacy), *Shreya Singhal* (online speech), and *Vishaka* (sexual harassment).

The statutory framework is examined across the Information Technology Act 2000, the Bharatiya Nyaya Sanhita 2023, and the Protection of Children from Sexual Offences Act 2012, revealing significant definitional gaps, overlapping provisions, and interpretive inconsistencies that undermine their protective effectiveness. The IT (Intermediary Guidelines) Rules 2021 are evaluated for their adequacy in regulating platform accountability, with the study finding meaningful progress offset by uneven implementation and the absence of an independent enforcement authority.
The central finding is that despite formal legislative comprehensiveness, online harassment persists at escalating rates due to chronic under-resourcing of cybercrime investigation, institutional hostility toward women victims, and fragmented jurisprudence across jurisdictions.

Reform recommendations include enacting a comprehensive Online Safety Act, establishing an independent Digital Safety Regulator, building specialist law enforcement capacity, codifying a right to erasure for harassment victims, and enacting a dedicated Children's Online Safety Act. These reforms are proposed as constitutional imperatives necessary to ensure India's digital transformation is equitable and rights-respecting for its most vulnerable citizens.

.

INTRODUCTION

Online life now shapes how people connect, turning the web into a space where daily activities like shopping, learning, dealing with officials, and building friendships happen. Smartphones spread fast in India, phone data got way cheaper after 2016 thanks to Jio, and national programs pushed digital tools harder this mix helped build one of the biggest, quickest expanding internet crowds on Earth. By 2024, more than 900 million Indians were online; experts expect over a billion soon. Still, wider reach brings darker outcomes harassment online is exploding, hitting women and kids hard no matter their income level, location, or schooling.

What happens online can hurt just like anything offline. When someone keeps sending threats through messages or posts, that counts. Following another person too closely across apps and websites often isn't curiosity it becomes something darker. Posting private details like addresses or phone numbers without permission is done on purpose to cause trouble. Pictures meant to stay hidden sometimes appear where they shouldn't, shared by people who ignore boundaries. Mocking, shaming, or shutting others out in games or comment sections repeats until it wears down the target. Fake profiles pretending to be someone else twist trust into confusion. Altered images made to humiliate spread fast and linger longer than anyone wants. Younger users face even sharper risks when unwanted advances arrive disguised as friendly talk. Fear builds slowly through comments, tags, emails, pings. Each method uses tech differently yet aims at one thing control through discomfort.

It starts with old imbalances control shaped by tradition, the reducing of people to bodies, unequal standing these forces existed long before screens, now they stretch further through wires. When women in India speak up whether in newsrooms, on stages, inside legislatures, or classrooms attacks follow, not random ones, but planned waves meant to wear down presence, discredit truth, push retreat from online view. Reports from groups like the National Commission for Women and the Internet Freedom Foundation show clear trends: threats laced with sex-based harm target women far more often, private pictures get spread without permission, mob like targeting intensifies pressure. Young users confront risk because growth leaves gaps in judgment, awareness of danger comes slow, while grown predators move fast behind hidden names, using distance and disguise to coax, lure, collect, circulate illegal imagery.

Online bullying laws in India come from many different rules, court decisions, and government actions that do not always fit together well. Though updated in 2008, the core law remains the Information Technology Act of 2000, covering things like dirty content posted online, spying through devices, threats sent digitally, and explicit material involving children. Because of how judges have interpreted it, older offenses under the 1860 penal code such as watching someone without consent, spreading lies, scaring people, or harassing others sexually are now applied when they happen on the internet; most of these are now part of the new Bharatiya Nyaya Sanhita introduced in 2023. Then there is the 2012 law meant only for kids the Protection of Children from Sexual Offences Act, later tightened in 2019, which works alongside tech regulations to handle serious cases where young ones face harm online. Back in 1986, a law meant to stop indecent portrayals of women didn't mention computers or phones. Still, courts later decided it applies to images online too. That widened what counts as protection. Jump ahead to 2021, new rules for internet companies began demanding stricter checks on user content. These steps aim at reducing how easily abuse spreads across digital spaces. Platforms now carry more responsibility when harmful material slips through.

This work dives into how laws actually function, using court rulings and real world enforcement to map out protections against digital abuse targeting women and children across India. Because dignity matters alongside freedom from sexual harm and full involvement in society the absence of strong safeguards online weakens constitutional promises rooted in Articles 14 through 21. When harmful behaviour spreads without consequences in digital spaces, rights erode quietly; thus legal systems must step in not just because they can, but because they should. Close readings of legislation meet historical context here, layered with evolving global norms on tech related threats tied to gender and youth risks. Insights build slowly not through sweeping claims but by questioning existing rules, past decisions, and fresh ethical directions shaping justice ahead.

REGULATORY FRAMEWORK: INTERMEDIARIES, PLATFORMS, AND ENFORCEMENT MECHANISMS RELATED TO ONLINE HARASSMENT

The regulation of social media intermediaries and digital platforms constitutes the frontier of online harassment law the domain where the law must grapple most directly with the structural reality that the primary sites of online harassment are privately owned, globally operating, technologically sophisticated platforms that exercise enormous power over the digital public sphere while operating largely outside the traditional regulatory frameworks designed for public broadcasting, public utilities, or public spaces. India's approach to intermediary regulation has evolved significantly through successive iterations of the Information Technology (Intermediary Guidelines) Rules, from the 2011 Rules through the landmark 2021 Rules, reflecting a progressive legislative recognition that the passive, conduit-based model of intermediary liability that dominated the early internet era is inadequate to address the scale and systemic nature of online harm in the age of algorithmic amplification and mass social media participation.

THE SAFE HARBOUR REGIME: SECTION 79 IT ACT AND ITS LIMITATIONS

Section 79 of the Information Technology Act, 2000 provides the statutory foundation of the 'safe harbour' or 'mere conduit' immunity that intermediaries enjoy from liability for third-party content. The provision states that an intermediary shall not be liable for any third-party information, data, or communication link made available or hosted by it if: the intermediary's function is limited to providing access to a communication system over which the information is transmitted, the intermediary does not initiate the transmission, select the receiver, or select or modify the information contained in the transmission, and the intermediary observes the due diligence and other guidelines prescribed. The Explanation to Section 79 defines 'intermediary' broadly to include any person who on behalf of another person receives, stores, or transmits electronic records or provides any service with respect to such records.

The safe harbour protection of Section 79 is conditional on compliance with the due diligence requirements specified in the IT (Intermediary Guidelines) Rules. Where an intermediary fails to fulfil these requirements, it loses its immunity and becomes directly liable for third-party content hosted on its platform. The Supreme Court in Shreya Singhal v. Union of India (2015) considered the constitutional validity of the obligation imposed by the 2011 Rules on intermediaries to take down content upon receiving a court order or government direction, and upheld the provision to the extent that it required compliance with court orders, while striking down the requirement of compliance with government directions without judicial oversight as disproportionate and unconstitutional. The Court's holding in Shreya Singhal established the important principle that the safe harbour immunity is not absolute and can be conditioned on the fulfilment of procedurally fair and constitutionally sound due-diligence obligations.

The practical limitations of Section 79's safe harbour regime as a mechanism for protecting women and children from online harassment became apparent in the years following the enactment of the 2011 Rules. Platforms routinely failed to take timely action on complaints of harassment, citing the volume of content, the difficulty of distinguishing harassing from legitimate expression, and the absence of clear legal standards for content moderation. The reporting mechanisms available to victims were inadequate, opaque, and unresponsive. The complaint resolution processes lacked transparency, consistency, and procedural fairness. And the absence of any regulator with clear authority to oversee and enforce intermediary compliance meant that safe harbour immunity functioned in practice as a shield against accountability rather than as a balanced allocation of responsibility between platforms and users.

IT (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the 2021 Rules), notified under Sections 87(2) and 79(2) of the IT Act, represent the most significant regulatory development in Indian cyberlaw since the 2008 Amendment and have generated substantial legal, policy, and constitutional controversy. The 2021 Rules introduce the category of 'Significant Social Media Intermediary' (SSMI) defined as a social media intermediary that has registered users in India above a threshold notified by the Central Government (currently 5 million users) and impose substantially more rigorous obligations on SSMIs than on ordinary intermediaries. The Rules require all intermediaries to publish detailed privacy policies and user agreements in accessible language, to establish grievance redressal mechanisms with specific timelines for complaint resolution, and to cooperate with law enforcement requests in accordance with legally specified procedures. SSMIs are additionally required to appoint Indian-resident Nodal Officers, Grievance Officers, and Chief Compliance Officers; to publish periodic compliance reports; to enable identification of the 'first originator' of end-to-end encrypted messages in specified circumstances; to provide a mechanism for victims of certain categories of harmful content (including non-consensual intimate imagery) to seek expedited content removal; and to deploy automated tools for the proactive identification and removal of child sexual abuse material.

The 2021 Rules' provisions on expedited removal of non-consensual intimate imagery are of direct significance for the protection of women from online harassment. Rule 3(2)(b) requires intermediaries to establish a mechanism for users to report content that depicts 'nudity or sexual act, morphed images etc.' without consent and to resolve such complaints within 24 hours. This represents a significant improvement over the 2011 Rules, which did not prescribe specific timelines for complaint resolution in non-consensual intimate imagery cases and did not distinguish between different categories of harmful content requiring different response urgency. The practical implementation of this provision has, however, been uneven: the largest platforms have established dedicated reporting mechanisms that are reasonably accessible, while smaller and medium-sized platforms have frequently failed to establish any such mechanism or have provided one that is technically available but practically dysfunctional.

The traceability requirement under Rule 4(2) of the 2021 Rules which requires SSMIs that provide end-to-end encrypted messaging services to enable identification of the 'first originator' of a message chain on receipt of a government order issued by specified authorities has been among the most constitutionally contentious provisions of the Rules. The provision has been challenged by WhatsApp and multiple civil society organizations before the Delhi High Court on the grounds that it violates the constitutional right to privacy (Puttaswamy), is technically incompatible with genuine end-to-end encryption, and would require platforms to retain metadata in a manner that creates surveillance infrastructure susceptible to abuse. Defenders of the provision argue that it is necessary for the investigation of online harassment and other cybercrime, since anonymous communication channels are frequently used by harassers to evade identification, and that the judicial oversight mechanism built into the rule provides adequate constitutional protection. The constitutional validity of Rule 4(2) remains contested and has not been definitively resolved by the Supreme Court.

THE NATIONAL CYBER CRIME REPORTING PORTAL AND INSTITUTIONAL ENFORCEMENT

The National Cyber Crime Reporting Portal (NCRP), launched by the Ministry of Home Affairs under the Indian Cyber Crime Coordination Centre (I4C) framework, represents the primary institutional mechanism for receiving and processing complaints of cybercrime including online harassment. The portal allows victims to file complaints online and tracks their forwarding to the relevant police jurisdictions for investigation. A dedicated sub-portal for cybercrime against women and children reporting.cybercrime.gov.in provides a simplified complaint mechanism specifically designed for these categories of victims, with provisions for emergency response in cases of child sexual abuse material. The portal has received millions of complaints since its launch, with a significant proportion relating to online harassment, financial fraud, and CSAM.

Despite the existence of the NCRP, the institutional effectiveness of cybercrime investigation and prosecution in India remains severely constrained by resource limitations, technical capacity deficits, jurisdictional coordination challenges, and attitudinal barriers. The National Crime Records Bureau's data on cybercrime consistently shows very low charge-sheeting rates and conviction rates relative to the number of complaints received, reflecting the gap between formal institutional capacity and actual investigative performance. Research by the Internet Freedom Foundation and the Centre for Communication Governance has documented systematic patterns of complaint refusal and delayed registration at police stations, particularly in cases involving women victims

of online harassment, attributable to the cultural stigmatization of sexual harassment, the low priority assigned to cybercrime cases in police station resource allocation, and the inadequacy of training in digital evidence collection and preservation.

CONCLUSION

The internet was supposed to be a great equaliser a space where geography, background, and social standing mattered less, and where anyone could speak, connect, and participate on equal terms. For millions of women and children in India, that promise remains unfulfilled. Behind the remarkable numbers 900 million internet users and counting lies a quieter, more troubling reality: that for a significant portion of those users, going online means navigating fear, harassment, and harm that the law has been slow to address and institutions even slower to remedy.

This study has traced the contours of that gap with care. India does not lack laws. The Information Technology Act, the Bharatiya Nyaya Sanhita, POCSO, and the Intermediary Guidelines of 2021 together form a framework that, on paper, is reasonably comprehensive. Courts have affirmed constitutional protections. Policies have been revised. Portals have been launched. And yet, women continue to be driven off platforms by coordinated abuse, children continue to be groomed and exploited behind encrypted screens, and survivors continue to encounter police stations where their complaints are dismissed or quietly shelved. The problem, in short, is not purely legislative it is institutional, cultural, and structural.

What has emerged clearly from this analysis is that legal text alone cannot carry the weight of protection. Section 79 of the IT Act created safe harbour for platforms that, in practice, often functions as a shield against accountability. The 2021 Rules improved grievance timelines for non-consensual intimate imagery but left implementation uneven and enforcement toothless. The National Cyber Crime Reporting Portal processes millions of complaints, yet conviction rates remain dismally low a statistic that reveals not the absence of law but the absence of will, training, and resources to enforce it.

The constitutional imperative is not abstract. Articles 14, 15, 19, and 21 guarantee equality, dignity, free expression, and privacy. When online harassment silences women from newsrooms, legislatures, and public debate, or when a child's exploitation circulates unchecked on a platform for days before removal, these guarantees are violated in spirit if not always in letter. The judiciary has moved thoughtfully Puttaswamy anchored privacy, Shreya Singhal refined speech protections, but judicial intervention alone cannot substitute for systemic reform.

The recommendations flowing from this research are not radical; they are proportionate responses to documented failures. A dedicated Online Safety Act would consolidate fragmented provisions into a coherent, enforceable framework. An independent Digital Safety Regulator would end the present situation where no single authority holds platforms genuinely accountable. Specialist cybercrime units staffed with trained investigators would begin closing the gap between complaints filed and justice delivered. A codified right to erasure would restore some dignity to survivors. A Children's Online Safety Act would treat child protection online with the seriousness it deserves.

India is building a digital future at extraordinary speed. The question this research leaves open and urgent is whether that future will be built for everyone, or only for those already powerful enough not to need its protection.

REFERENCE

1. *Justice K S Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (Supreme Court of India) (https://main.sci.gov.in/judgment/judis/45418.pdf)

2. *Shreya Singhal v Union of India* (2015) 5 SCC 1 (Supreme Court of India) (https://indiankanoon.org/doc/110813550/)

3. *Vishaka v State of Rajasthan* (1997) 6 SCC 241 (Supreme Court of India) (https://indiankanoon.org/doc/1031794/)

4. Information Technology Act 2000 (India), ss 66A, 66E, 67, 67A, 67B, 79 (https://www.indiacode.nic.in/handle/123456789/1999)

5. Protection of Children from Sexual Offences Act 2012 (India), as amended by Protection of Children from Sexual Offences (Amendment) Act 2019 (https://www.indiacode.nic.in/handle/123456789/2079)

6. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rr 3, 4 (India) (https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf)

7.Bharatiya Nyaya Sanhita 2023 (India), ss74,75,79 (https://www.indiacode.nic.in/handle/123456789/20062)

8. Pavan Duggal, *Cyberlaw: The Indian Perspective* (Saakshar Law Publications 2022) (https://www.saaksharlawpublications.com/cyberlaw-the-indian-perspective)