SEXUALIZATION, ONLINE HARASSMENT AND BLACKMAIL: THE VULNERABILITY OF YOUNG WOMEN ON INDIAN SOCIAL MEDIA PLATFORMS

Pallavi Soni*

ABSTRACT

The survey shows popular social media websites such as Facebook, Instagram, Snapchat, WhatsApp, and Tinder, young Indian women are more susceptible to sexualization, online abuse and blackmail. The negative aspects of online participation have attracted considerable attention, especially for teenage girls and women, due to the rapid growth of internet access and digital activity. This study examines how certain platform-specific features, such as algorithmic content promotion, media, anonymous messaging, and disappearing from local moderation, can enable a culture of digital abuse and exploitation. Changes in identity and image-based abuse. Surprisingly, the systematic failure of women's digital security in 2022, in the rise in cybercrime, is determined by 24.4%. The inadequate digital forensics and the shame associated with reports of such crimes. Expert comments and NGO results show that stronger accountability is needed through high-tech platforms, digital literacy initiatives and sacrifice-centric political reform. This study concludes with specific suggestions for safer online rooms, including the positive moderation of Indian language, educational initiatives, localised security technologies, and the need for a strong response to legal remedies. Finally, this study highlights how important it is to recognise online gender-specific violence as a public emergency and advocate for the rights of young women in India's changing digital environment.

Keywords: Social Media, Online Harassment, Sexualization, Cybercrime against Women.

*BA LLB, FOURTH YEAR, GALGOTIAS UNIVERSITY, GREATER NOIDA.

INTRODUCTION

India has seen an exponential increase in internet usage, which has given people there, especially the young, unprecedented access to digital platforms, particularly among the country's youth. According to the Indian Report 2022 by IAMAI and KANTAR[1], it estimates that there were 759 million internet users in the nation in 2022, with that figure expected to rise to 900 million by 2025. As of early 2025, women constitute approximately 33.1% of Instagram users in India and on Facebook, women account for 33.5%.

In terms of age demographics, the majority of female social media users fall within the 18-24 and 25-34 age brackets. Social media platforms like Facebook, Instagram, Snapchat, WhatsApp, Tinder and others have ingrained themselves firmly into young women's social lives. However, a troubling trend, a startling increase in sexualization, online harassment, and blackmail, has been brought about by this digital integration.

The Indian Penal Code and the Information Technology Act, 2000 both have cyber provisions, but their implementation is still disjointed and mostly insensitive to the gender-specific characteristics of online abuse. 83% of the urban Indian women, according to a 2023 survey,[2] feel uncomfortable online since image-based abuse, stalking, and blackmail have become commonplace on these sites. However, legal remedies like platform accountability and FIRs are either inaccessible or poorly executed. This study looks at how India's legal system handles online harassment, blackmail, and non-consensual content, among other digital damages against women. Data, case law, and expert opinions are used to illustrate enforcement gaps, the function of tech platforms, and the pressing need for reform in order to guarantee equality, dignity and digital safety.

CONCEPTUAL FRAMEWORK

The key terms and concepts to provide clarity and structure to the research:

[1] Internet and Mobile Association of India and KANTAR, Internet in India Report 2022 (3 May 2023) https://www.moneycontrol.com/news/business/internet-users-in-india-set-to-reach-900-million-by-2025-report-10522311.html accessed 7 May 2025

[2] Business Today, '8 in 10 Urban Indian Women Use the Internet, But Face Harassment, Abuse, Trolling Online: Survey' (8 March 2023) https://www.businesstoday.in/latest/trends/story/international-womens-day-2023-8-in-10-urban-indian-women-uses-internet-struggle-with-harassment-abuse-trolling-says-report-372662-2023-03-08 accessed 7 May 2025.

Sexualization: The act of representing or treating women in sexual terms, often without their consent or context. On social media, this includes unsolicited sexual messages, manipulated images, or the framing of women's identities in sexual ways to attract attention or provoke responses.

Online Harassment: A form of cybercrime that involves repeated or targeted digital behaviours such as trolling, stalking, abuse, or threats intended to intimidate, harm, or humiliate individuals. It often includes the use of social media, messaging apps, and digital forums.

Digital Blackmail: The use of personal, often sexual, content (sometimes obtained without consent) to coerce or threaten individuals for monetary gain, sexual favours, or continued silence. This is growing cybercrime against young women in India.

Gendered vulnerability in digital spaces: Women face disproportionate online risks due to societal gender norms and weak regulation.

THE ROLE OF INSTAGRAM IN FACILITATING SEXUALIZATION, BLACKMAIL, AND HARASSMENT

How can the sexualization and exploitation of young women occur on a platform intended for self-expression and connection? Although Instagram was created as a medium for self-expression and creativity, it has evolved into a digital environment where young Indian women are subjected to sexual exploitation and objectification. Users, particularly women, are under indirect pressure to adhere to performative beauty and sexual ideals because of the platform's algorithm-driven emphasis on visual appeal and interaction, which tends to promote hyper sexualized content.

A frightening 94% of female Instagram influencers have been the victim of deepfake pornography, according to a 2024 study by Twicsy.[3]. The risk increases as the influencer's following grows; for every 10,000 followers, the risk rises by 15.7%. Targeting is more common in industries like fashion, entertainment, and beauty, where female influencers are 85%, 82%, and 81% more likely to be targeted, respectively. In total, 84% of social media

[3] DAU Secretariat, 'Twicsy: 84% of Social Media Influencers Fall Victims to Deepfake Pornography' (DAU, 24 June 2024) https://dau.mcaindia.in/blog/84-of-social-media-influencers-fall-victims-to-deepfake-pornography accessed 7 May 2025

influencers, 90% of whom are female, have purportedly been the victims of deepfake pornography.

This kind of sexualized content has a significant psychological influence.[4]. About 50% of teenage girls, according to research in the Indian Journal of Social Psychiatry, report being unhappy with their bodies. This percentage is significantly greater than the 31% recorded for boys. Internalising the unrealistic beauty standards promoted by social media is linked to this discontent, which lowers self-esteem and raises body image issues. Despite current legislation such as the Information Technology Act, 2000 and sections 354A and 354D of the Indian Penal Code, victims frequently face restricted access to legal remedy, law enforcement indifference, and platform inaction. The legal system is made even more complex by the absence of laws specifically targeting deepfake pornography, which deprives many victims of sufficient protection and legal channels.

BLACKMAIL AND HARASSMENT ON INSTAGRAM: THE DIGITAL ENTRAPMENT OF YOUNG WOMEN

Instagram's promise of self-expression and digital community has, in many cases, taken a darker turn, particularly for young women in India. Features such as appearance-focused algorithms, anonymous interactions, and the prevalence of fake profiles have made the platform a breeding ground for harassment, blackmail and sexual extortion. These platform dynamics not only expose women to digital threats but also contribute to deep psychological and emotional distress, making them vulnerable to exploitation within what is often perceived as a safe social space.

A report from Snap Inc. and CyberPeace Foundation in 2024 indicated that 71% of polled Indian Gen Z users have encountered or been targeted by online sextortion, predominantly via platforms such as Instagram and Snapchat.[5] Instagram blackmail frequently takes a similar pattern: the criminal gains trust through seemingly harmless exchanges, takes private or intimate photos, and then turns these into a weapon by threatening to make the photos public

[4] Manisha Singh Palawat and others, 'Social Media's Seductive Spell: Unraveling the Impact on Adolescent Body Image' (2024) 40(4) Indian Journal of Social Psychiatry 341 https://journals.lww.com/ijsp/fulltext/2024/40040/social_media_s_seductive_spell___unraveling_the.3.aspx accessed

[5] Snap Inc., '55% of Indian Gen Z Fell Victim to Sextortion in 2024: Snap Study' (Campaign India, 3 February 2025) https://www.campaignindia.in/article/55-of-indian-gen-z-fell-victim-to-sextortion-in-2024-snap-study/500608 accessed 10 May 2025.

unless more are sent or money is paid. Many young women do not report these crimes because they are afraid of social stigma or reprisals.

A well-known instance from Delhi (2023) was a 16-year-old girl who was tricked into revealing private information by a phoney influencer account, blackmailed for months, and finally sought assistance. The case attracted a lot of attention and demonstrated how slowly law enforcement tracked down and eliminated exploitative content.

Instagram has added a few safeguards, including limiting undesired interactions (e.g., blocking and filtering messages). Turning off screenshots for communications that vanish. Alerts for questionable behaviour, like a bot account that follows a lot of people. Partnerships with child safety NGOs such as India's CyberDost, the National Centre for Missing and Exploited Children (NCMEC), and Thorn. However, many users find these tools confusing, especially those who are not familiar with digital safety procedures, and they are frequently underpublicized. Furthermore, damaging content can spread quickly before action is taken because of algorithmic biases that enhance inflammatory content and a lack of localised moderation.[6]

WHY ARE INDIAN WOMEN INCREASINGLY VULNERABLE TO ONLINE HARASSMENT AND BLACKMAIL ON FACEBOOK?

In recent years, the digital landscape in India has seen a significant surge in online harassment and blackmail targeting women, primarily on platforms like Facebook. Despite increased internet access among women, these platforms have become breeding grounds for cybercrimes due to various socio-cultural and technological factors.

Facebook's Role in Facilitating Abuse: Facebook's vast user base and features like anonymous profiles and private messaging have inadvertently facilitated the spread of harassment and blackmail. A study by BOOM Live revealed that Indian women often face severe threats on Facebook, with perpetrators operating freely due to inadequate moderation, especially in regional languages.

Societal Stigma and Underreporting: Cultural norms and fear of social ostracisation contribute to the underreporting of online harassment. Many women choose to remain silent

[6] Instagram, 'Protecting Teens from Online Harm' (Instagram Blog, 17 October 2024) https://about.instagram.com/blog/announcements/campaign-against-teen-sextortion accessed 7 May 2025.

about reporting due to concern about family reputation and lack of awareness about legal recourse. Women often face backlash for expressing opinions online, leading to self-censorship and withdrawal from digital platforms.

HOW DOES SNAPCHAT CONTRIBUTE TO THE RISING THREAT OF SEXTORTION AND ONLINE HARASSMENT AGAINST WOMEN IN INDIA?

Snapchat, a platform celebrated for its Transitory messaging and creative filters, has become a mixed blessing for women in India. While it offers free ways for self-expression and anonymity, it also exposes users to significant risks, including sextortion, grooming, and unauthorised dissemination of intimate content. Recent studies and reports highlight the growing concerns surrounding women's safety on this platform. Snapchat's disappearing messages and screenshot-blocking features, while originally intended to increase privacy, often work against victims. These functionalities allow predators to send unsolicited explicit content or coerce intimate media from victims, knowing there is limited evidence left behind. However, Snapchat does not require name registration, allowing users to create fake or anonymous profiles with ease, facilitating impersonation and deception.

REAL LIFE CASES OF SOCIAL MEDIA EXPLOITATION AGAINST WOMEN IN INDIA

1. The Exploitation Scheme of an Interior Designer Based in Delhi. A 32-year-old interior designer was detained by Delhi Police in February 2023 for sexually abusing young ladies and stalking them on Instagram. To trick males into sharing pictures of their female friends, the accused made several fictitious profiles, pretended to be a young woman, and then utilised the women's private images as a form of blackmail.[7]

2. Blackmail Techniques Used by Hyderabad Engineering Students A 19-year-old Hyderabadi engineering student was arrested in January 2024 for using Instagram to stalk and extort women. To blackmail victims, he made a phoney profile, pretended to be a girl, and forced them to share private images, which he later altered into pornographic material.[8]

[7] Delhi-Based Interior Designer's Exploitation Scheme' NDTV (New Delhi, 21 February 2023) https://www.ndtv.com/india-news/delhi-based-interior-designer-arrested-for-stalking-sexually-harassing-girls-on-instagram-3817781 accessed 18 May 2025

[8] Hyderabad Engineering Student's Blackmail Tactics' The Times of India (Hyderabad, 4 January 2024) https://timesofindia.indiatimes.com/city/hyderabad/engineering-student-held-for-stalking-blackmailing-women-on-instagram/articleshow/106529159.cms accessed 18 May 2025.

3. The Experience of a Bengaluru Woman with Instagram Friendship A 37-year-old Bengaluru woman confided in a man she befriended on Instagram about her marital issues. Later, the man threatened to release the naked pictures and videos she had provided, extorting her for cash and gold. She was kicked out of her house after he called her husband and told him about the affair.[9]

4. A woman from Bhopal was blackmailed via a phoney Facebook account. A 21-year-old married woman from Bhopal was blackmailed in November 2021 by an unidentified person who made phoney Facebook and Instagram accounts in her name. She was blackmailed with having her pornographic photos posted online unless she paid ₹5 lakh. She complained to the cybercrime section when the pictures were uploaded after she disregarded the threats.[10]

5. A man was arrested for using Facebook to morph and blackmail women. A 26-year-old Keralan man was arrested in Delhi in June 2019 for taking Facebook photos of girls, turning them into nude photos, and then using the photos to blackmail the victims. By threatening to release the altered photos, he demanded money. The defendant acknowledged utilising the funds for personal needs and debt repayment.[11]

6. The image of the Udupi teen was distorted and shared on Snapchat. A snapshot of a 14-year-old girl was altered into a pornographic film and shared on a phoney Snapchat account in Udupi, Karnataka, in July 2023. By Sections 66C and 67(B) of the Information Technology Act, the occurrence prompted a police inquiry.[12]

7. A Bengaluru man uses Snapchat videos to blackmail women. In March 2024, 24-year-old Bengaluru resident Arjun Gowda was arrested for forcing women to post naked videos on Snapchat. Using these unconsented recordings, he blackmailed people for cash and sexual

[9] Bengaluru Woman's Ordeal with Instagram Acquaintance' The Times of India (Bengaluru, 3 May 2024) https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-woman-falls-victim-to-instagram-blackmail-disturbing-details-unfold/articleshow/115062249.cms accessed 18 May 2025.
[10] 'Bhopal: 21-Year-Old Woman Blackmailed on Social Media' Times of India (Bhopal, 20 November 2021) https://timesofindia.indiatimes.com/city/bhopal/bhopal-21-year-old-woman-blackmailed-on-social-media/articleshow/87501453.cms accessed 18 May 2025.
[11] Man Held for Blackmailing Girls after Morphing Their Facebook Pics' Business Standard (Delhi, 5 June 2019) https://www.business-standard.com/article/news-ians/man-held-for-blackmailing-girls-after-morphing-their-facebook-pics-119060501078_1.html accessed 18 May 2025.
[12] Woman Files Complaint after Daughter's Morphed Video Is Posted on Snapchat in Udupi' The Hindu (Udupi, 2 August 2023) https://www.thehindu.com/news/cities/Mangalore/woman-files-complaint-after-daughters-morphed-video-is-posted-on-snapchat-in-udupi/article67147402.ece accessed 18 May 2025.

favours. According to investigations, he had taken advantage of at least six other women in a similar manner.[13]

8. The Snapchat Incident in the Boys Locker Room Snapchat was linked to the 2020 "Boys Locker Room" investigation, which involved the distribution of pornographic photos of minors. Investigations showed that indecent chats were started using a phoney Snapchat profile, sparking indignation and conversations about online safety.[14]

EXPERT PERSPECTIVES ON THE DIGITAL RISKS FACING YOUNG WOMEN ON SOCIAL MEDIA

UNESCO's Findings on Social Media's Impact on Girls' Well-being and Education: A UNESCO report warns that algorithm-driven, image-based content on social media exposes girls to material ranging from sexual content to videos glorifying unhealthy behaviours or unrealistic body standards. This exposure negatively affects girls' self-esteem and body image, impacting their mental health and academic success. The report cites Facebook's research, which found that 32% of teenage girls felt worse about their bodies after using Instagram. Additionally, girls suffer more cyberbullying than boys, with 12% of 15-year-old girls reporting being cyberbullied compared to 8% of boys.[15]

Meghan Markle on Online Harassment and the Need for Digital Safety: Meghan Markle, the Duchess of Sussex, shared her experiences of peak online abuse and bullying during her pregnancies. Speaking at the SXSW Conference, she discussed the cruelty she faced online and her decision to distance herself from social media for her well-being. Markle emphasised the challenges new mothers face, exacerbated by unrealistic portrayals of motherhood on social media, and highlighted the need for online safety and support for women and new mothers.[16]

---

[13] Bengaluru Man Blackmails Women Using Snapchat Videos' The Times of India (Bengaluru, 27 March 2024) https://timesofindia.indiatimes.com/city/bengaluru/man-held-for-blackmailingwomen-with-their-nude-pix/articleshow/108831323.cms accessed 18 May 2025

[14] Ananya Bhardwaj, 'Delhi Police Clears Girl Who Created Fake Snapchat Profile and Started "Rape Talk"' ThePrint (Delhi, 12 May 2020) https://theprint.in/india/delhi-police-clears-girl-who-created-fake-snapchat-profile-and-started-rape-talk/422494 accessed 18 May 2025.

[15] New UNESCO Report Warns Social Media Affects Girls' Well-being, Learning and Career Choices' UNESCO (11 October 2023) https://www.unesco.org/en/articles/new-unesco-report-warns-social-media-affects-girls-well-being-learning-and-career-choices accessed 18 May 2025.

[16] 2. Escher Walcott, 'Meghan Markle Says Online Bullying Peaked during Her Pregnancy, Calls for Better Digital Safety' People (8 March 2024) https://people.com/meghan-markle-online-bullying-peaked-pregnancy-prince-archie-princess-lilibet-sxsw-panel-discussion-international-womens-day-8606548 accessed 18 May 2025.

THE ROLE OF SOCIAL MEDIA PLATFORMS: STRUCTURAL LOOPHOLES AND SYSTEMIC FAILURES IN PROTECTING WOMEN FROM HARASSMENT, BLACKMAIL, AND SEXUALIZATION

Major social media companies like Facebook, Instagram, Snapchat, WhatsApp, and Tinder have made claims to be concerned about user safety, but they have continuously failed to address the systemic risks that women and girls, particularly in India, face. The primary goal of these platforms is engagement and growth, and as a result, they often put user growth and revenue generation ahead of proactive content moderation and safety enforcement, creating environments where abuse can flourish with little repercussion.

Algorithmic Amplification and Design Bias: Visual and sensational content are frequently given priority by platform algorithms, which can subject women to increased scrutiny, objectification, and sexualization. For example, it has been demonstrated that Instagram's Explore feed and hashtag systems disproportionately amplify appearance-based posts, especially those from young women, making them prime targets for predators. The Wall Street Journal's 2023 investigation found that Instagram's recommendation system deliberately led children into loops of sexually exploitative content, a trend that cyber safety NGOs in India have verified. Similarly, despite being designed for privacy, Snapchat's disappearing messages and screenshot notifications have been used as weapons by criminals. Perpetrators frequently force young women to share explicit content to use it for sextortion. However, Snapchat's moderation systems are still ill-equipped to identify and address these situations promptly.

Loopholes in Policy Enforcement: Platforms enforce their community standards inconsistently, particularly in regional languages and contexts that deviate from Western norms. According to reports by Amnesty International and the Mozilla Foundation, Facebook and Instagram do not have enough content moderators who speak Indian languages, which causes them to respond to abuse reports in a timely or accurate manner. Furthermore, victims frequently have no recourse due to the opaque appeals procedures. Safety flaws are more noticeable on WhatsApp and Tinder. Because Tinder's verification features are optional, identity-based fraud and catfishing are permitted. WhatsApp's encrypted messages make it difficult for authorities or even the platform to step in without a user report because they are commonly used to share non-consensual content in closed groups.

T**he Lack of Localised Safety Infrastructure:** For Indian users, many platforms lack culturally relevant tools such as regional language safety centres, automated moderation that is trained in Indian slang or code words, and easy access to cyber police channels. Even when the tools are available, this reduces their effectiveness.

LEGAL FRAMEWORK IN INDIA ADDRESSING ONLINE HARASSMENT AND BLACKMAIL AGAINST WOMEN

Through the Information Technology Act of 2000 (IT Act), the Indian Penal Code (IPC), and some particular amendments, India has formulated a legal mechanism to deal with cybercrimes, especially those related to women. These laws seek to control various types of virtual stalking, cyberbullying, extortion, and sexploitation. Nevertheless, issues regarding enforcement and education continue to exist.

Information Technology Act, 2000 -

The IT Act provides provisions to address cyber offences:

Section 66E: Punishes violation of privacy by capturing, publishing, or transmitting images of private areas without consent.

Section 67: Criminalises publication or transmission of obscene material in electronic form.

Section 67A: Sexually explicit material; invoked often in revenge porn or sextortion cases.

Section 66C & 66D: Identity theft & impersonation using electronic means applicable in catfishing & fake profiles.[17]

Indian Penal Code (IPC) -

The IPC includes provisions relevant to online harassment:

Section 354D: Addresses cyberstalking, where a man follows or contacts a woman repeatedly despite clear disinterest.

Section 509: Deals with words, gestures, or acts intended to insult the modesty of a woman, including online messages.

[17] Information Technology Act 2000, ss 66C, 66D, 66E, 67, 67A.

Sections 499 & 500: Cover defamation, applicable to harmful and false content shared on social media.

Section 292: Prohibits the sale and publication of obscene material.[18]

Criminal Law (Amendment) Act, 2013 -

Enacted in response to the 2012 Nirbhaya case, this Act expanded definitions of sexual harassment and assault to include online behaviours:

Section 354A: Defines sexual harassment, including unwelcome physical contact, advances, and sexually colored remarks.

Section 354C: Introduces voyeurism as an offence, penalising the act of watching or capturing images of a woman engaging in a private act without consent.

Section 354D: Reiterates stalking, encompassing monitoring a woman's use of the internet, email, or any other form of electronic communication.

These provisions aim to protect women's privacy and dignity in both physical and digital spaces.[19]

Protection of Children from Sexual Offences (POCSO) Act, 2012

The POCSO Act provides a comprehensive legal framework to protect children from offences of sexual assault, sexual harassment, and pornography:

- It criminalises online grooming, image-based abuse, and the transmission of pornographic content involving children.
- The Act mandates the reporting of such offences and prescribes stringent punishments to deter potential offenders.[20]

[18] Indian Penal Code 1860, ss 292, 354D, 499, 500, 509.
[19] Criminal Law (Amendment) Act 2013, ss 354A, 354C, 354D
[20] Protection of Children from Sexual Offences (POCSO) Act 2012.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

These rules impose obligations on intermediaries, including social media platforms, to ensure user safety:

Grievance Redressal Mechanism: Intermediaries must appoint a Grievance Officer to address user complaints within specified timelines.

Content Removal: Platforms are required to remove or disable access to content exposing private areas, depicting nudity or sexual acts, or impersonation, within 24 hours of receiving a complaint.

Traceability: Significant social media intermediaries must enable the identification of the first originator of information on their platforms under certain conditions.

Compliance Officers: Appointment of Chief Compliance Officer, Nodal Contact Person, and Resident Grievance Officer, all of whom must be residents of India. [21]

CHALLENGES AND LOOPHOLES IN LAW ENFORCEMENT AND THE JUSTICE SYSTEM

Though India boasts a robust legal structure about cybercrimes against women, systemic issues, technological limitations, and societal barriers often come in the way of the proper implementation of laws. These are problems that greatly impede the journey of victims towards justice in cases of sexual exploitation, blackmail, and abuse online.

Underreporting Due to Social Stigma: Underreporting proves to be a major hindrance in the fight against cybercrimes towards women. Due to cultural conventions, most women refrain from complaining and this also, to a greater extent, does not want to damage their reputation. In most cases, the victims are scared of social ostracism, being blamed for the crime against them, or even backlash from their families; this silence gives the perpetrators a free hand.

Lack of Digital Literacy and Awareness: A significant number of women and girls in India, particularly from semi-urban and rural areas, are unprepared to exercise digital literacy or take

[21] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

advantage of legal remedies that are available to them. This unpreparedness is exploited by offenders participating in blackmail, sextortion and impersonation.

Inadequate Police Training and Sensitisation: Police officers frequently lack the technical expertise necessary to conduct thorough investigations into cybercrimes. Additionally, victims are deterred from seeking assistance since police officers are not often gender sensitive. Managing concerns responsively is a complex procedure; an insensitive approach may result in case pulling or retraumatization.

Delays in Judicial Process: The trial and resolution of cybercrime cases in India are drastically delayed because of the overloaded court system. The lengthy processes, multiple court appearances, and slow collection of digital evidence deplete victims' confidence in the system.

Loopholes in Legal Definitions and Jurisdiction: At times, the current legislation is vague or simply overlooks the new and evolving shapes of online abuse (for example, doxing and deepfakes). Prosecution becomes increasingly complicated due to cross-jurisdictional issues occurring when servers or perpetrators are offshore in another country. For example, when dealing with overseas platforms, revenge porn cases can be complicated by the lag associated with international cooperation and data sharing.

Ineffective Grievance Redressal by Platforms: Although laws in India require platforms to have grievance redressal systems, the vast majority of social media companies fail to even have timely responses or robust support in local languages. Victims often receive automated responses or experience unreasonable delays in the removal of content.

RECOMMENDATIONS

Because of the increasing safety and dignity risk posed to young women in India by social media platforms, a multi-layered approach that combines legal, educational, technological, and sociological measures is essential. The recommended policies outlined will build upon the prevention, defence, and prosecution of some cases of sexual exploitation, blackmail, and harassment that take place via the internet:

1. **Strengthen Platform Accountability:** Implement more stringent guidelines under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which require Facebook, Instagram, Snapchat, Tinder, and other platforms

to: Within 24 hours, remove any reported hazardous information. Support regional languages in procedures for resolving grievances. Use AI-powered moderating tools that are considerate of regional cultural norms. Require transparency reports that include information on enforcement activities, response timelines, and abuse situations.

2. **Enhance Digital Literacy for Women:** Include modules specifically designed for girls in school and college curricula to teach digital safety. Start national initiatives to educate women and their families about online privacy and consent. Protocols for reporting cybercrimes. Social media safety procedures.
3. **Police Reforms and Capacity Building:** Teach police officers gender-sensitive investigation tactics and cyber forensics. Create specialised cybercrime squads in each district, staffed by female officers. Simplify online complaint processes (e.g., by making the 1930 helpline and cybercrime.gov.in more functional).
4. **Legal Reforms and Fast-Track Courts:** Extend the IT Act's definition of cyber harassment to cover new dangers like doxxing, deepfakes, and AI-generated nudes. To guarantee prompt justice, establish fast-track tribunals for cybercrimes based on gender. Encourage judicial officers who handle instances involving digital violence to undergo obligatory cyber training.
5. **Community and Institutional Support:** Universities should set up campus-based digital safety cells to assist students who are being harassed online. Urge NGOs and civil society organisations to provide victims with counselling, legal assistance, and rehabilitative support.

CONCLUSION

In India, the digital revolution has opened up a plethora of opportunities for empowerment, self-expression, and connection, especially for young women who are increasingly vocal on the internet. However, the very platforms that provide visibility and independence have also become spaces of trauma, control, and exploitation. This research has shown how technological errors, inadequate content regulation, and deeply ingrained gender biases often facilitate harassment, sexualization, and extortion on various social networking platforms such as Facebook, Instagram, Snapchat, WhatsApp, and Tinder.

Numerous reports from the national crime records bureau and media investigations have revealed a significant rise in cybercrime incidents, underscoring the structural weaknesses of digital infrastructure and legal frameworks in protecting vulnerable individuals. Real-life

incidents demonstrate grooming, image-based abuse, and manipulative behaviours that disproportionately affect young women and girls and are often concealed by institutional indifference, shame, and stigma.

Despite the existence of laws such as the POCSO Act, the it Act, and IPC provisions, the execution of these laws remains slow, disjointed, and ill-equipped to address the ever-evolving risks associated with the internet. Victims lack faith in the legal system, law enforcement agencies are inadequately trained, and tech platforms prioritise user engagement over security measures.

Nevertheless, this paper also emphasises the potential for alteration. India can establish a digital environment that respects women's rights, independence, and self-worth by enacting targeted modifications to legislation, educational curricula, and online platform structures, while also promoting awareness at the local level and establishing support systems for victims. Safeguarding young women in the digital realm is a social imperative that underscores our collective dedication to justice, equality, and the principles of digital democracy; it is not solely a matter of policy.