



INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

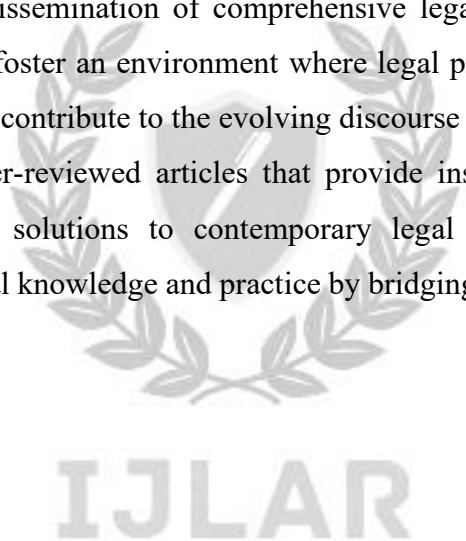
DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.



Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

FROM STALKING TO DEEP FAKES: REGULATING CYBER VIOLENCE IN THE DIGITAL AGE – A KERALA PERSPECTIVE

AUTHORED BY – ASWIN JOSHY P

Designation- L.L.M. Scholar IPR and Cyber Laws

Educational Qualification- 4th Semester LLM Scholar

Affiliated Institution – School of Indian Legal Thought, Mahatma Gandhi University

Abstract

Cyber violence against women has grown rapidly with the advancement in digital technology, taking forms such as stalking, deepfakes, morphed imagery, sextortion, and coordinated online harassment. While constitutional guarantees and statutory law provide some protection, existing legal frameworks remain largely unenforced and inadequate, leaving perpetrators unaccountable and victims without meaningful redress. This paper aims to study how cyber violence systematically erodes women's safety, dignity, and autonomy in digital spaces using a doctrinal and comparative methodology. The paper examines regulatory responses across the European Union, Australia, the United Kingdom, and the United States, and compares them with the Indian context.

In India, while privacy is recognised as a fundamental right following *Justice K.S. Puttaswamy v. Union of India*. No specific legislation exists governing social media, non-consensual deepfakes, or platform liability for gender-based digital violence. The paper uses Kerala as its primary case study, evaluating the state's institutional mechanisms, including the Cyberdome, the Gender Help Desk, and the Kerala Women's Commission. The paper concludes by identifying key regulatory gaps and proposing reforms to strengthen platform accountability, criminalise AI-specific offences, and harmonise consent protections with the right to free expression.

Keywords: Cyber violence, women's digital safety, deepfakes, platform liability, AI-generated abuse

1. Introduction

In today's modern world, the internet is one of the most powerful sources of information and support, which helps people connect across the globe by making the world feel like a global village. The internet has created many opportunities for people, such as online jobs, banking, websites, social movements, and communication with others. It has allowed people to freely share their ideas and thoughts. The Internet has encouraged discussions, activism, and different forms of debate. Various social media platforms, such as Twitter, Facebook, and dating apps, help people interact with others and be part of a larger community. Online places can be unfriendly and harsh at times.

The Digital age has witnessed unprecedented growth in cybercrime. The nature of violence shifted with the digital age. The traditional “violence” refers to the physical harm or direct verbal abuse. The harm in the digital age has evolved beyond spaces into online environments by giving rise to so-called cyber violence. In cyber violence, the harm is inflicted using digital technologies. Through social media, a harmful post or video that can reach thousands or millions instantly. Once the online content is posted, it is very difficult to remove it entirely. The offenders usually hide their identity, making accountability harder. Advances in artificial intelligence have made it easier to create fake audio and video of people. Deepfakes have targeted celebrities and commoners as well. The AI tools are easily accessible and free, enabling the creation of realistic synthetic images. It's extremely scary that the fake images created are being used in pornographic videos.

From 2021 to 2025, cybercrime complaints against women nearly doubled, from 1.24 lakh to 2.5 lakh.¹ The major categories of cybercrimes included fake profiles and impersonation, identity theft, sexually obscene content, cyberbullying, stalking, sexting and sextortion. The complaints related to child sexual abuse material increased.

The 2023 Deepfake video of Indian actress Rashmika Mandanna exposed a major gap in India's legal system, as there were no specific laws addressing deepfakes and AI-generated abuse. BNS was insufficient to address the rising tide of cybercrime.²

¹ Vismay Basu, *Cybercrimes against Women Go up in 5 Years*, THE NEW INDIAN EXPRESS (Mar. 23, 2026), <https://www.newindianexpress.com/india/2026/Mar/23/cybercrimes-against-women-go-up-in-5-years>.

² *Rashmika Mandanna Calls for Action against “scary” Deepfake Video*, Nov. 7, 2023, <https://www.bbc.com/news/world-asia-india-67305557>.

The existing literature has overlooked the need for a detailed, jurisdiction-specific examination of how cyber violence can be controlled. The current laws are outdated, as they were designed for a different era and struggle to keep pace with the scale, speed, and complexity of modern cyber violence.

To investigate these issues rigorously, this research adopts a mixed-methods approach that combines doctrinal and empirical approaches. The doctrinal analysis involves a careful reading of primary sources, including legal statutes, judicial decisions, and regulatory guidelines, along with empirical methods to understand how these laws function in practice.

2. Literature Review

Danielle Keats Citron's Hate Crimes in Cyberspace

(2014). In her book, she argues that cyber harassment is not merely a free speech issue but a serious civil rights problem that causes real harm. Women are especially targeted in cyber harassment, which includes threats, privacy invasion, reputational damage and online attacks. Existing laws are inadequate as they do not address anonymous or group-based violence. Citron proposes updating the laws to include online harassment, stalking and penalising non-consensual content like revenge porn. Citron suggested that Online platforms should be held accountable rather than given full immunity, and victims should be protected through anonymity in legal cases.³

Bacher -Hicks A, Goodman J, Green JG, Holt MK. The COVID -19 pandemic disrupted both school bullying and cyberbullying. Am Econ Rev Insights. 2022;4(3)353. The study provides a crucial insight that the physical school environment is often the primary engine for offline and online abuse. In schools, these types of behaviours originate and interact with one another. During initial lockdowns, there was a 30% to 40% reduction in search interest for bullying-related terms. The online bullying depends on the school environment and peer groups⁴.

³ *Hate Crimes in Cyberspace*, HARVARD UNIVERSITY PRESS, <https://www.hup.harvard.edu/books/9780674659902> (last visited July 26, 2026).

⁴ *The COVID-19 Pandemic Disrupted Both School Bullying and Cyberbullying - American Economic Association*, <https://www.aeaweb.org/articles?id=10.1257/aeri.20210456> (last visited July 26, 2026).

Kaur & Saini (2023) “Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions”. The author evaluates the efficacy of various Indian government programs aimed at curbing digital harassment. Higher education institutions are significant hubs for cyberbullying due to the high internet penetration among students. The paper indicates a sharp rise in cybercrime in India from 2018 to 2019, with a 63.8% increase, a trend that continued in 2020. The primary finding of the study is that awareness of existing legal protections and reporting mechanisms is low among both students and faculty. The Author advocates for Digital literacy for students about safe and responsible internet use as part of the curriculum. There should be student support systems and dedicated helplines to deal with cyberbullying.⁵

A Study on Awareness Regarding Cyberbullying among Students in Cochin City. This study aims to gain a general understanding of cyberbullying and to assess the level of awareness among college students in Cochin City, Kerala. The target population was 60 respondents, college students from different colleges in Cochin city. The study looked at how cyberbullying affects victims across three dimensions, such as mental, emotional and physical. The victims faced low self-esteem, anger, embarrassment, shame, loss of interest, sleep loss, headaches and stomach issues. It also looked at awareness of response mechanisms, whether the affected students know how to respond to cyberbullying by seeking help from trusted adults, reporting bullies, preserving evidence, and contacting authorities. The study found that cyberbullying is linked to suicidal ideation in extreme consequences.⁶

Narrative Review on Indian Adolescents- In this study, the impact of cyberbullying on Indian adolescents was assessed. Cyberbullying is increasing due to rising tech access, social media, poor awareness and prevention measures. The severe psychological and physiological effects, such as depression and stress-related health issues, are associated with cyberbullying. During Covid 19, the cyberbullying trends increased due to prolonged online exposure. It also calls for coordinated government action to protect adolescents.⁷

⁵ Manpreet Kaur & Munish Saini, *Indian Government Initiatives on Cyberbullying: A Case Study on Cyberbullying in Indian Higher Education Institutions*, 28 EDUC INF TECHNOL 581 (2023).

⁶ Liya Xavier, *A Study on Awareness Regarding Cyber Bullying among Students in Cochin City*.

⁷ *Silent Screams: A Narrative Review of Cyberbullying Among Indian Adolescents* | Cureus, <https://www.cureus.com/articles/269362-silent-screams-a-narrative-review-of-cyberbullying-among-indian-adolescents#!/> (last visited July 26, 2026).

Navigating the Digital Landscape: Understanding Cyberbullying, Its Impacts and Strategies for Prevention. This literature identifies a transition from traditional bullying to sophisticated “AI-mediated” abuse. The key behaviours discussed include brigading, common trolling, and Doxing. The research shows that cyberbullying has serious psychological and social impacts, which include low self-esteem, anxiety, depression, academic decline, substance use and increased suicidal ideation. Evidence shows that students use technical coping and social support by seeking help from friends and family rather than resorting to retaliation.⁸

Coping Strategies and Psychological Wellbeing Among Undergraduate Students Experiencing Cyberbullying: A Cross-Sectional Study. This study focused on cyberbullying as an emerging concern among undergraduate students since online interactions have become part of daily college life. The researchers wanted to examine the link between cyberbullying and psychological well-being. For the study, 744 undergraduate students aged 18 to 24 were surveyed out of 800. The study found 86.02% of female participants, with a mean age of 20.41, who use 5.08 hours of the internet per day. The 40.32% were victims of cyberbullying, where 25.5% admitted to perpetrating cyberbullying and 32.25% were both victims and perpetrators. The technical coping, like blocking or reporting, was most common, second most common was social support, and Retaliation was the least common.⁹

LEGAL FRAMEWORK AND ITS LIMITATIONS

The IPC and BNS in the Era of Deepfakes and Digital Harm

The Indian Penal Code was written in 1860¹⁰ long before the internet, social media, or AI. Since there was no single piece of legislation that directly addressed Deepfake videos and AI-generated fake images, police had to piece together different sections like forgery, defamation, and outraging the modesty of women. This mainly weakened and slowed cases. Bharatiya Nyaya Sanhita requires proving intent, deception, or harm. The rise in deepfakes makes it difficult to prove who created the content and whether it was meant to harm. The BNS has only

⁸ Bhaswatty Das & Nurnahar Ahmed, *Navigating the Digital Landscape: Understanding Cyberbullying, Its Impacts, and Strategies for Prevention*, KERALA JOURNAL OF PSYCHIATRY (2026), <https://kjponline.com/index.php/kjp/article/view/569>.

⁹ Md Adil Faizan et al., *Coping Strategies and Psychological Wellbeing Among Undergraduate Students Affected by Cyberbullying: A Cross-Sectional Study*, 38 KERALA JOURNAL OF PSYCHIATRY 115 (2025).

¹⁰ The Indian Penal Code, 1860 (Act No. 45 of 1860).

updated the IPC numbering and missed the opportunity to update the nature of the crime.¹¹ The IPC was drafted to address physical, face-to-face crimes, not complex digital crimes in today's world.

In BNS, there are several modernised provisions relevant to cyber violence, but it still has gaps. The modern issues, like Deepfake pornography¹² Organised online harassment, like trolling in the groups, sextortion for money or favours, is not dealt with under the law.

Stalking is defined under Section 354D of the IPC. It requires repeated contact from a single source. In the digital world, a stalker uses 10 different throwaway accounts to harass a victim 10 times, making the law ineffective against anonymous, multi-account cyberstalking.¹³

Defamation is defined under Section 499 of the IPC. It is a slow, procedural process in which the police cannot act without a magistrate's order. The Deepfakes go viral in minutes, and the damage is permanent. By the time you get a court order, the content has already gone viral. The IPC lacks mechanisms for rapid takedown, making it ineffective against viral content.¹⁴

Protection of women from domestic violence act 2005

Before the enactment of the Protection of Women from Domestic Violence Act 2005, there was no specific civil law in India to address domestic violence; the victims could only use Section 498 IPC and Section 125 CRPC. The Protection of Women from Domestic Violence Act 2005 was mainly drafted with the aim of protecting women from domestic violence. The act mainly focuses on physical abuse, emotional or verbal abuse, and economic abuse. When this act was passed in 2005, digital abuse was not explicitly covered by the law, as it wasn't a major legal concern at the time.¹⁵

Breakdown of Chain of Custody in Digital Evidence

In *Xxxx v. State of Kerala & ors*, the case shows a systematic challenge in Kerala against the inadequate procedural safeguards in the collection, handling and preservation of digital evidence in sexual assault and intimate image cases. In this case, mis-handling of sexually explicit digital evidence led to the unauthorised access, potential leakage, and erosion of victim

¹¹ The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

¹² Ritik Agrawal, *DEEPFAKE AND AI CRIMES IN INDIA: THE URGENT NEED FOR A STRONG LEGAL FRAMEWORK*, JUS SCRIPTUM (Jan. 31, 2026), <https://www.juscriptumlaw.com/post/deepfake-and-ai-crimes-in-india-the-urgent-need-for-a-strong-legal-framework>.

¹³ Indian Penal Code 1860, (Act 45 of 1860), s.354 D.

¹⁴ Indian Penal Code 1860, (Act 45 of 1860), s.499.

¹⁵ The Protection of Women from Domestic Violence Act 2005, (Act 43 of 2005).

privacy and dignity protected under Article 21. This also undermines the fairness of trials and weakens the overall justice system in cyber cases. When digital evidence is seized, its hash value is generated. Even if a single bit of the file changes, the hash value changes completely. In this case, the hash value of the memory card containing sexually explicit evidence under the court's custody was changed. This shows serious systemic failure in digital safe handling. The victims are facing further harm beyond the original crime, which undermines trust in the criminal justice system. Due to the repeated exposure, victims face psychological and reputational harm, which reduces the willingness of victims to report cyber offences.

The State-Level Data Vacuum

The central government publishes national cybercrime statistics that include cases against women through the NCRB and other Agencies, but those figures are not broken down by state for 2025 in any publicly accessible official report. The 2025 data on cybercrime against women in Kerala remains unpublished or aggregated into border national tables.

The NCRB's annual crime in India report for 2024 is still awaited and is expected only in late 2026. This clearly shows a nearly 2-year lag between the crime year and the official publication of data. The state-level 2024 data are not yet available in a standardised, official format. Without timely state-level data, it is very difficult to measure the scale and pattern of cybercrime against women in Kerala, like stalking, non-consensual sharing of intimate images, fake profiles, OTP fraud, and cyber stalking.

The data gap can be categorised as a transparency and accountability issue. It is the duty of the central and state governments to publish state-wise disaggregated data on cybercrime against women within a defined time frame. The data that hides behind timely delays indirectly protects perpetrators and weakens victims' claims because, without visible statistics, the problem can be dismissed as anecdotal rather than structural.

When the government fails to fully meet its obligations under international agreements, a human rights failure has occurred. The International agreements include the Convention on the Elimination of All Forms of Discrimination Against Women and the Beijing Platform for Action. These frameworks do not just require governments to make laws against violence against women. They also require the governments to track the problem by collecting data, understanding patterns and reporting it publicly. When Kerala does not publish clear, detailed state-level data on cybercrime against women, laws and policies cannot be effectively designed without such data. The Government cannot be questioned or evaluated without proper data.

The lack of data is not an accident but a failure to act on a legal obligation.

Typology of Cybercrime Against Woman

Cyber Bullying

Cyber Bullying is a form of repeated harassment, humiliation or intimidation through digital platforms like social media, messaging apps or emails. When a group repeatedly posts abusive comments and body-shaming messages on a woman's Instagram, it amounts to cyberbullying. The Person engaged in cyberbullying intends to harass, threaten or humiliate by using electronic communication, causing emotional distress to the victim. Many victims of cyberbullying use blocking, reporting, privacy settings and help from friends or family instead of retaliation¹⁶.

Cyber Stalking

Cyber stalking is rising, and women are the most likely targets. In cyber stalking, the internet is used to stalk someone for online abuse and harassment. A Cyber stalker monitors, tracks, or harasses a woman online without engaging in a direct threat to the victim. It creates fear or distress for the victim.

Cyber Defamation

Cyber Defamation involves publishing false or harmful statements about a woman online to damage her reputation. If a person posts false allegations about a woman's character on social media or other platforms causing social stigma. The victim's reputation is targeted.

Cyber Morphing

Cyber morphing involves editing the original picture by an unauthorised user or a fake identity. The woman's photos are morphed into explicit images and uploaded to fake social media accounts. The created images are often used in a sexual or defamatory manner to harm the dignity and reputation of the victim.

From Delhi, a 21-year-old man was arrested for allegedly using AI tools to morph a college student's photo into explicit images, which were uploaded through fake social media accounts created in the victim's name, and this showed how AI is being used to intensify online harassment, sexual abuse and defaming a woman online.¹⁷

¹⁶ Jorge Casaña Mohedo et al., *Study of the Relationship Between Cyberbullying and Mental Health in Adolescents-A Systematic Review*, 13 CHILDREN (BASEL) 367 (2026).

¹⁷ *Delhi Man Arrested For Morphing Woman's Photos, Uploading Them Online*, <https://www.ndtv.com/india-news/delhi-man-arrested-for-morphing-womans-photos-uploading-them-online-8813829> (last visited July 26, 2026).

Cyber Trolling

Cyber Trolling involves posting offensive, abusive or provocative comments to harass or emotionally disturb a woman online. If a woman expressing her opinion online is targeted with abusive comments, rape threats and hate messages.

The Tamil Nadu Cyber Crime wing arrested a woman for creating AI-generated obscene images of a senior employee from her former workplace and circulating them to her colleagues through fake IDs on Instagram. She downloaded the victim's photograph from the company's official website and used an artificial intelligence application to morph images into obscene content. The fake accounts created to distribute the manipulated, defamatory images targeted the senior employee. The investigators traced the accused by analysing digital footprints and online activity. The accused used social media to threaten the victim, harass her, publicly humiliate her and damage her professional reputation. This case shows that AI tools can be misused to create non-consensual manipulated images that harm an individual's reputation.¹⁸

LANDMARK JUDGEMENTS ON CYBERCRIME AGAINST WOMEN

State of Tamil Nadu v. Suhas Katti (2004)¹⁹

The Accused Suhas Katti had harassed a divorced woman by posting her phone number and defamatory messages on a public message board about the victim. The messages were published in a Yahoo message group and other online forums. The victims received obscene calls from strangers. This was India's first-ever conviction under the IT Act.

Avinash Bajaj v. State (NCT of Delhi)²⁰

In this case, an obscene MMS clip was listed for sale on the website Baazee.com. The CEO, Avinash Bajaj, was arrested and charged. This case sparked a massive debate about intermediary liability.

Kalandi Charan Lenka v. State of Odisha (2017)²¹

The Accused in this case created a fake Facebook profile in the victim's name. He then posted morphed and obscene photographs of her and sent sexually explicit messages to her friends and

¹⁸ Chennai: Woman Arrested for Using AI to Create Obscene Photos of Senior at Former Workplace, https://www.dtnext.in/news/chennai/chennai-woman-arrested-for-using-ai-to-create-obscene-photos-of-senior-at-former-workplace?utm_source=chatgpt.com (last visited July 26, 2026).

¹⁹ State of Tamil Nadu v. Suhas Katti, C No. 4680 of 2004.

²⁰ Avinash Bajaj v. State (NCT of Delhi), (2005) 3 Comp LJ 364 (Del).

²¹ Kalandi Charan Lenka v. State of Odisha, MANU/OR/0027/2017.

family, ruining her social reputation and causing mental agony. The Odisha High Court refused to grant bail to the accused, highlighting the extreme depravity of the crime. The court said that using technology to damage a woman's character is a serious offence. The Court recognised that morphed images and fake profiles constitute a severe violation of a woman's right to live with dignity under Article 21 of the Constitution.

State of West Bengal v. Animesh Boxi (2017)²²

In this case, the accused shared private photos and videos of his partner online without her consent when their relationship ended. The applied section 66E of the Information Technology Act 2000, which deals with violation of privacy. It was one of the first cases in India that was convicted for "revenge porn". The case showed that sharing private images online without consent amounts to a serious crime. The court also recognised the serious emotional and psychological harm caused to the victim.

XXXX v. State of Kerala & Ors²³

In this Case, the Court took Cognisance of the Unauthorised access to a memory card containing sexually explicit content that had been kept in the court's custody. The prosecution raised concerns that the content had been copied and transmitted via digital platforms, including Telegram, WhatsApp, and Instagram, without authorisation. The Kerala High Court held that this constituted a serious violation of the victim's privacy and fundamental rights. The court also noted that no one is permitted to access court evidence without proper legal permission. The court ordered an inquiry into how the leak happened.

CASE STUDIES AND SOCIETAL IMPACT

In Kerala, cybercrime cases are increasing dramatically, from 77 cases in 2022 to 3295 in 2023 alone. The number of crimes registered against women in the state also rose from 13,539 cases in 2021 to 16,025 in 2023.²⁴

The cybercrime complaints involving women in India rose significantly in 2025, reaching over 76,657 cases on the NCRP, an increase of nearly 28,000 from 2024. The offences included

²² State of West Bengal v. Animesh Boxi, C.R.M. No. 11806 of 2017.

²³ XXXX v. State of Kerala & Ors., WP(Crl.) No. 445 of 2022(ker).

²⁴ Kerala Sees Rise in Crimes Against Women, Cyber Offences, Murder, Onmanorama, Oct. 1, 2025, available at: <https://www.onmanorama.com/news/kerala/2025/10/01/kerala-crime-statistics> (last visited on April 21, 2026).

serious offences such as online harassment, stalking, and the circulation of obscene and exploitative content-related complaints, forming the largest share. According to data presented in the Rajya Sabha, cybercrime incidents reported to the NCRO have shown a sharp upward trend, rising from 4.52 lakh in 2021 to 2.3 million in 2026.²⁵

From Achievement to Abuse:- The Cyber Trolling of Prachi Nigam

According to the cybercrime cases reported through the National Cybercrime Reporting portal, the data reveal an even steeper escalation. Cybercrime complaints surged by 148%, rising from 9619 cases in 2022 to 31,019 by mid-2024. The findings by law enforcement authorities noted that women constitute a primary target group of cyber offences in the state.²⁶

Even harassment happens to high-achieving girls in India. The example of Prachi Nigam, 2024 UP Board class 10 topper, who faced cyber trolling for her facial hair after her phone went viral following her outstanding score of 98.5%. From this example, we can see that, instead of celebrating her achievement, people mocked her facial hair on social media. Many social media users posted memes and insulting comments about her, abusing her, ignoring her academic success.²⁷

Nigam drew on the example of Chanakya, who was historically trolled for his appearance, to argue that great minds are often targeted and that this did not affect him; similarly, she pointed out that the trolls did not affect her.

Digital Abuse and Its Lethal Impact: The Case of Athira in Kerala

In May 2023, Athira VM, a 26-year-old woman from Kottayam, committed suicide after facing continuous online harassment from her former partner, Arun Vidhyadharan. After their breakup, Arun threatened her repeatedly, shared her private photos and messages online without her consent and tried to damage her reputation on social media. Athira had already complained to the police, saying the harassment by Arun was severely affecting her life. But instead of stopping the abuse reportedly got worse.

Athira's death highlights serious failures in how digital abuse is handled. Athira had reported

²⁵ Lok Sabha, *GOVERNMENT OF INDIA MINISTRY OF HOME AFFAIRS*.

²⁶ *Cybercrimes Surge 148%: Women's Safety at Risk | Thiruvananthapuram News - The Times of India*, <https://timesofindia.indiatimes.com/city/thiruvananthapuram/cybercrimes-surge-148-womens-safety-at-risk/articleshow/114743703.cms> (last visited July 26, 2026).

²⁷ *Prachi Nigam, UP Board Topper Shuts down Trolls with Her Powerful Statement | - Times of India*, <https://timesofindia.indiatimes.com/life-style/health-fitness/de-stress/prachi-nigam-up-board-topper-shuts-down-trolls-with-her-powerful-statement/articleshow/109661164.cms> (last visited July 26, 2026).

the abuse, yet no timely action stopped it. The help was sought but not delivered. The private image was used as the weapon in this case. The Non-consensual sharing has caused humiliation and fear. The Gap in police response shows that the Delay between the complaint and action had tragic consequences. The system here failed to act when harm was already visible.²⁸

The Thiruvanthupuarm Influencer Case

An 18-year-old student from Thiruvanthupuram, known as Madhu, was an active Instagram creator with a growing following. She was described by her teachers as confident and ambitious, and as interested in becoming a cosmetologist. She was already earning a small income through her social media. She attempted suicide on June 10 and died on June 17, 2024. She has faced heavy online abuse after a rumoured breakup with her 21-year-old male friend. She had undergone heavy slut shaming and moral policing by her followers.

The social media platforms failed, as the abusive comments were public and visible. The harassment continued unchecked. The abuse was happening in plain sight. She was blamed and faced slut shaming for the breakup.²⁹

Kerala's Response to Cyber Violence

The Kerala Cyberdome is one of the most advanced cybercrime units in India, working with technology experts, companies, and law enforcement to tackle cyber threats. The Digital Forensics Lab can detect deepfakes, preserve social media evidence, and monitor data web activity.

Women can report Cybercrime online without visiting a police station through the Gender Help Desk (2019). It handled over 18,000 complaints by 2023, mostly related to cyberstalking and the sharing of private content. It also helped in removing harmful content and supports victims. The advanced methods are used to identify deepfakes under Cyberdome, which have been accepted as evidence in cases before the Kerala High Court.

The Kerala Women's Commission has actively addressed cyber violence by taking action on its own in several serious cases, issuing safety guidelines for social media platforms, and

²⁸ T. N. M. Staff, *Kerala Woman's Death over Cyber Harassment: Accused Found Dead in Hotel Room*, THE NEWS MINUTE (May 4, 2023), <https://www.thenewsminute.com/kerala/kerala-woman-s-death-over-cyber-harassment-accused-found-dead-hotel-room-176761>.

²⁹ *18-Year-Old Instagram Influencer Kills Self in Thiruvananthapuram, Cyber Bullying Alleged*, 18-YEAR-OLD INSTAGRAM INFLUENCER KILLS SELF IN THIRUVANANTHAPURAM, CYBER BULLYING ALLEGED, <https://www.onmanorama.com/news/kerala/2024/06/17/instagram-influencer-plus-two-student-suicide-poojapura-social-media-abuse.html> (last visited July 26, 2026).

publishing reports on digital violence.

Fragmented Regulation and Legal Vacuum: Challenges under the IT Rules 2021 and POCSO Act

Prachi Nigam's Example illustrates how cyberbullying disproportionately targets women and girls through appearance-based harassment, reflecting the deeper societal biases. She was subjected to widespread online trolling, which was focused on her physical appearance rather than her academic achievement and merit. The incident exposes a regulatory gap in both the Information Technology (Intermediary Guidelines) and the Digital Media Ethics Code Rules 2021, and the Protection of Women from sexual offences Act³⁰, as neither framework adequately addresses coordinated online harassment, body shaming or harmful digital harm happening in society. The IT Rules 2021 require intermediaries to remove unlawful content within 36 hours of receiving a notification and to appoint grievance officers to address user complaints. The IT Rules 2021³¹ are inadequate to address the harm in this case. These rules focus on detecting child sexual abuse material and previously flagged content. They do not require the platforms to identify or control non sexual harassment, body shaming, or coordinated trolling of minors. The viral abuse of this nature often goes unchecked, as in the case of Prachi Nigam.

RECOMMENDATIONS AND REFORMS

A standalone Kerala Cyber Violence Against Women Act

The most significant gap in the current legal architecture is the absence of a dedicated gender specific statute to address cyber violence against women. The Information Technology Act 2000, the Bharatiya Nyaya Sanhita 2023, and the POCSO Act together provided a fragmented and not designed to address the unique nature of online abuse.

The new act should clearly define cyber violence by including all forms of online harassment, cyberstalking, sharing private images without consent, deepfakes, doxxing, sextortion, fake profiles and AI-based abuse. The law should provide quick protection to victims, such as restraining orders or content removal, based on the complaint without waiting for a full trial. The law should hold social media platforms accountable.

³⁰ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

³¹ The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012)

A Dedicated kerala Cyber violence against women Authority

Kerala should create a special authority focusing only on cyber violence against women, separate from regular cybercrime units. The authority should have suo motu powers. The authority should work with the Cyberdome to detect harassment campaigns, fake accounts and morphed images early. It should support victims by providing free legal help, counselling, digital safety guidance, and assistance in removing harmful content.

Reforming Cyberdome

The cyberdome should be strengthened to place greater emphasis on women's online safety. It should create a Gender Cyber Safety Division with dedicated staff. A public real-time dashboard of cybercrime against women should be updated daily and maintained. The common threats like fake profiles, deepfakes and coordinated online abuse should be monitored. It should publish district-level risk reports to help police prevent cyber violence before it grows.

Mandatory state-level Cybercrime Reporting

The Kerala government should make it legally mandatory for the State Crime Records Bureau to publish a yearly report on cybercrime against women within six months of each year, which includes district-wise data on the number of complaints in each district, broken down by offence type. It should also include FIR conversion rates, charge sheeting rates, Trial outcome data, victim demographic data, and platform response data.

Education and Prevention- Digital Literacy for All

Prevention is the most effective solution. Kerala, with high literacy and strong education, should leverage its strong school and community networks. Digital rights should be added to the school curriculum starting in class 6. Students can learn about online consent, privacy settings, and how to report abuse. Cyber safety workshops be made mandatory for college students, as women aged 18 to 30 are the most frequent targets in deepfakes and sextortion cases.

Launching a statewide public awareness campaign on deepfake identification, consent in digital spaces, and reporting mechanisms.

Survivor -Centred support- Healing the Harm

Cybercrime causes deep emotional and social trauma, and Kerala needs a support system that

goes beyond just catching the hacker. The state should provide mental health support by providing free, private counselling for victims of cybercrimes through existing Women's Help Desks and One-stop centres.

Legal Mordernization

Kerala cannot fully amend national laws such as the Bharatiya Nyaya Sanhita 2023 or the Information Technology Act 2000. It can use its powers over police and public order to improve enforcement. The Kerala Law Commission and the state government can formally recommend to the central government that a dedicated deepfake offence be added to the IT Act or BNS. Stronger punishment for repeat and group offenders, since group harassment causes greater harm. The law should also punish those who knowingly share or forward private images or deepfake content. This helps in stopping secondary sharing.

Secure Digital Evidence Management System

The court should handle sensitive information and digital evidence with most care. The Data should have Encryption and Access control. The court should use a blockchain-based feature that tracks every access attempt. Strict chain-of-custody protocols should be followed. Sensitive evidence should use multi-factor authentication.

CONCLUSION

The fight against cyber violence is not only a legislative issue. It is about restoring human dignity online. It is about holding tech companies and those who weaponize their tools accountable for the damage they enable. We need to protect people -especially women from being silenced by threat, a morphed image or a coordinated mob long before any legal system steps in.

In the digital age, justice delayed is not justice denied. It is a life destroyed at the speed of a share button.