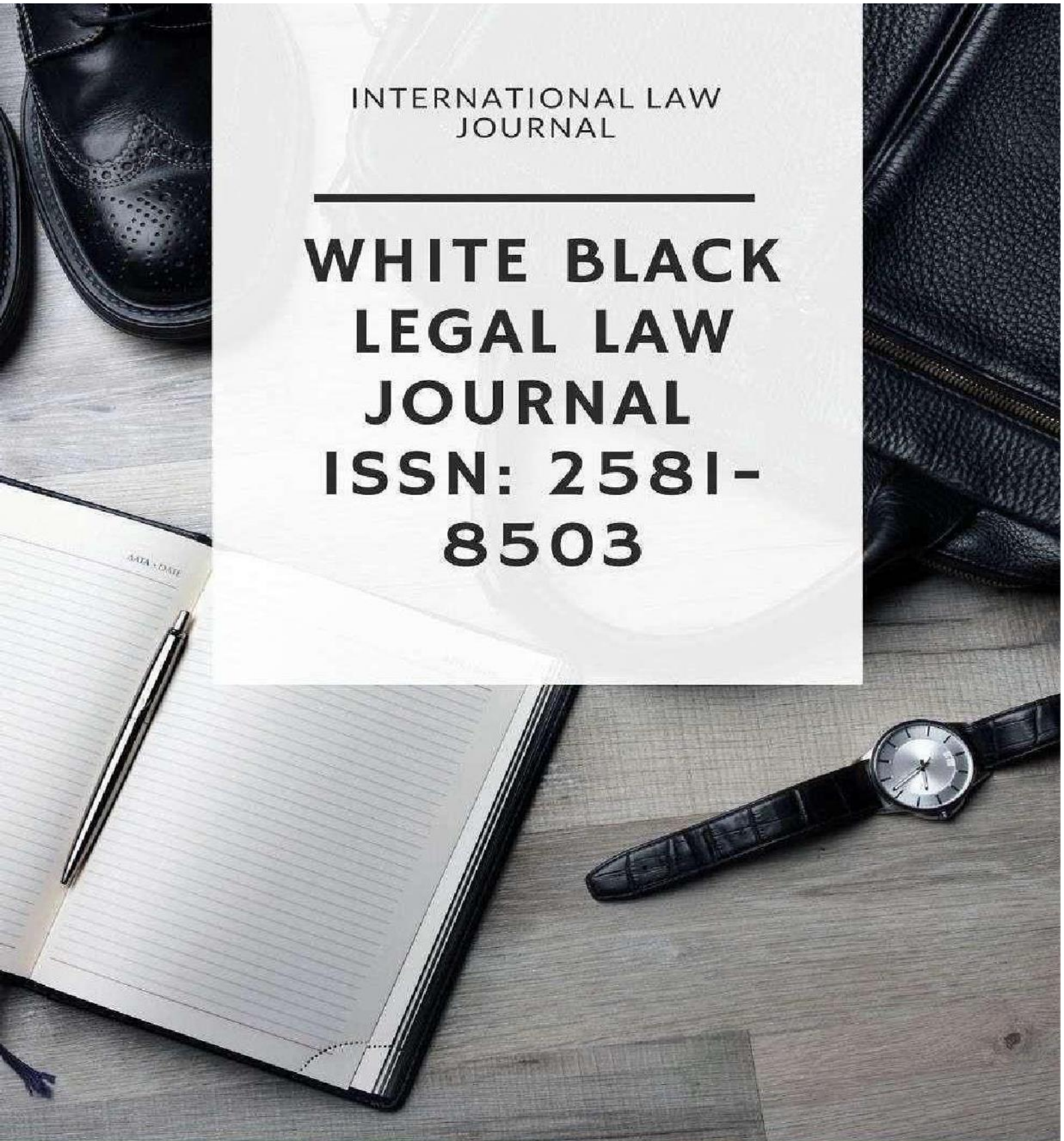




INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

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

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

WHITE BLACK
LEGAL

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

THE DOUBLE-EDGED SWORD OF TECHNOLOGY: HOW SOCIAL MEDIA FACILITATES CYBERBULLYING AND CYBER STALKING

AUTHORED BY - ADV. ANSHIKA YADAV

B.A.LL. B (Hons)

Advocate

TABLE OF CONTENTS

S.no	Title
I	DECLARATION
II	CERTIFICATE
III	TABLE OF CASES
IV	LIST OF ABBRIVIATION
1	CHAPTER- I:- INTRODUCTION
1.1	• Literature Review
1.2	• Statement of Problem
1.3	• Research question
1.4	• Objective
1.5	• Research Methodology
1.6	• Scope of Study
1.7	• Hypothesis
2	CHAPTER- II:- THE DIGITAL TERRAIN OF HARASSMENT UNDERSTANDING CYBERBULLYING AND CYBERSTALKING
2.1	• Detailed definitions and typologies of cyberbullying and cyberstalking
2.2	• How social media facilitates: ▪ Anonymity ▪ Amplification of harm
2.3	▪ Untraceable threats
2.4	• Victim profiles: children, women, LGBTQ+ individuals, influencers
2.5	

2.6	• Psychological and emotional consequences: depression, anxiety, suicide • Real-life Indian and global case examples
3	CHAPTER -III:- LEGAL AND FORENSIC FRAMEWORK IN INDIA
3.1	• Relevant Indian laws:
	• Information Technology Act, 2000 (Sections 66E, 67, 67A, 67B) • Indian Penal Code (Sections 354D, 507, 499, 500) • POCSO Act (for child victims)
3.2	• Judicial precedents
3.3	• Digital forensic investigation tools:
3.4	• Autopsy, FTK, Cellebrite, EnCase, etc.
3.5	• Challenges in evidence collection, jurisdiction, and data retrieval
3.6	• Role of cyber cells and digital forensic units
4	CHAPTER- IV:- PLATFORM RESPONSIBILITY AND COMPARATIVE ANALYSIS
4.1	• Role of platforms: Facebook, Instagram, Snapchat, Twitter/X, YouTube • Analysis of content moderation policies and transparency reports
4.2	• How tech features contribute to abuse (e.g., disappearing messages, encrypted DMs)
4.3	• Accountability gap: Safe Harbor protection vs. user safety • Comparative study:
4.4	▪ UK's Online Safety Bill ▪ USA's Stop Cyberstalking Bill (proposed)
4.5	▪ EU's Digital Services Act • Best practices and lessons for India
4.6	
5	CHAPTER- VI • CONCLUSION
7	BIBILIOGRAPHY

TABLE OF CASES

S.

No. Case Name Citation

2024 SCC OnLine Mad 11925

1 S. Harish S/o. Santhanam v. The Inspector of Police (India)

Just Rights for Children Alliance v. S. Harish & Ors. 2024 SCC OnLine Mad 11926 (India)

3 **Shreya Singhal v. Union of India** (2015) 5 SCC 1 (India)

Supreme Court Guidelines on Preventing Child

4 (2023) 6 SCC 519 (India)

Sexual Exploitation Material

5 **Avnish Bajaj v. State (NCT of Delhi)** (2005) 3 Comp LJ 364 (Del)

6 **K.S. Puttaswamy v. Union of India** (Right to Privacy

case)

6 (2017) 10 SCC 1 (India)

7 **Faheema Shirin R.K. v. State of Kerala** 2019 SCC OnLine Ker 31598

(India)

C.C. No. 4680/2004, Cyber

8 **State of Tamil Nadu v. Suhas Katti** Crime Court, Chennai

9 **Manik Taneja v. State of Karnataka** (2015) 7 SCC 423 (India)

XYZ v. Union of India (Facebook/WhatsApp tracing 2020 SCC OnLine SC 790

10 (India)

matter)

LIST OF ABBREVIATIONS

1.	IPC	Indian Penal Code
2.	SC	Supreme Court
3.	HC	High Court
4.	PIL	Public Interest Litigation
5.	CJI	Chief Justice of India
6.	US	United States of America

CHAPTER-I INTRODUCTION

Introduction

In the digital age, technology has transformed the fabric of human interaction. The proliferation of social media platforms has ushered in a new era of communication, collapsing geographical barriers and enabling real-time connectivity across the globe. Platforms like Facebook, Instagram, Twitter, WhatsApp, and Snapchat have evolved into virtual public spheres where individuals express themselves, form communities, build careers, and advocate for causes. For many, especially youth, social media has become an extension of their identity and social life. However, while these platforms have offered significant benefits in enhancing communication and access to information, they have also become instruments of harm, fostering new forms of abuse such as cyberbullying and cyberstalking. Cyberbullying refers to the use of digital platforms to harass, threaten, or humiliate individuals through repeated hostile behaviour. Cyberstalking, on the other hand, involves the persistent and unwanted surveillance, monitoring, or harassment of a person online. These phenomena are not mere extensions of traditional bullying and stalking; they are far more insidious due to the unique nature of the digital environment.

The anonymity afforded by the internet, the potential for rapid dissemination of harmful content, and the lack of immediate consequences embolden perpetrators and disempower victims. As a result, individuals especially minors, women, LGBTQ+ persons, and public figures are increasingly falling prey to digital violence, often with severe emotional, psychological, and even physical consequences.¹

In India, cyberbullying and cyberstalking have witnessed a steep rise in recent years, exposing gaps in legal protection, technological regulation, and forensic enforcement. While the Information Technology Act, 2000 and provisions of the Indian Penal Code do address certain aspects of online abuse, the legal framework remains fragmented, and enforcement

mechanisms are often inadequate. Forensic investigations are further complicated by the use of encrypted communications, VPNs, and fake accounts, making it difficult to trace and prosecute offenders. In this context, the question arises: How can the law and forensic science effectively respond to harms facilitated by platforms that were originally designed to connect and empower?²

This research paper explores the paradoxical role of social media as both a tool for empowerment and a breeding ground for online abuse. It examines how the structural and algorithmic features of social networking sites such as anonymous messaging, disappearing content, and lack of stringent moderation contribute to an environment conducive to cyberbullying and cyberstalking. It also analyses how victims are affected and how forensic technology, digital laws, and law enforcement agencies are currently equipped to respond to these challenges. The study adopts a qualitative doctrinal methodology supported by secondary data, including academic literature, case studies, news reports, judicial decisions, and platform policies. It aims to critically evaluate the existing legal and forensic responses to online abuse in India and compare them with best practices from other jurisdictions such as the United States, the United Kingdom, and the European Union.

The ultimate objective is to identify gaps in the current approach and propose practical reforms both legal and technological to strengthen the protection of individuals in the digital space. Given the increasing reliance on digital communication, addressing cyberbullying and cyberstalking is not just a matter of policy it is a matter of human dignity, public health, and social justice. As technology continues to evolve, so must our legal and ethical frameworks, to ensure that social media remains a tool for connection rather than a weapon of harassment. This research aspires to contribute to the broader discourse on cyber safety and digital rights by shedding light on the nuanced challenges posed by the darker side of social media.

1.1 Literature Review

1. **"A Review of the Research on Children and Young People Who Display Harmful Sexual Behaviour Online"**: This literature review by the NSPCC informs and updates guidance for practitioners working with children and young people displaying harmful sexual behaviour, including online child pornography³

2. **A Narrative Review of Cyberbullying Among Indian Adolescents**

This review highlights the rising incidence of cyberbullying among Indian adolescents, attributing it to increased access to technology and social media, coupled with insufficient awareness and prevention measures. The study emphasizes significant

gender differences in aggression patterns and underscores the severe psychological effects on victims, including depression and stress-related health issues.⁴

3. Cyberbullying on Social Networks A Crime in India

This paper discusses the various forms of cyberbullying prevalent on social networks in India, such as spreading rumors, posting hurtful comments, and sharing embarrassing content. It examines the legal standpoint, noting that cyberbullying may be considered a crime depending on the jurisdiction and severity of actions, and emphasizes the need for robust legal frameworks to address this issue.⁵

4. Cyberbullying and Cyberstalking: Their Influence on the Social and Emotional Development of Teenagers in India

This study explores how cyberbullying and cyberstalking profoundly affect the social and emotional development of Indian teenagers. It discusses the psychological effects, coping strategies, and preventive measures, highlighting the need for comprehensive interventions to safeguard adolescents' well-being.⁶

5. Cyberbullying Legislation in India: Effectiveness and International Comparisons

This paper examines India's existing legal framework addressing cyberbullying, analysing its effectiveness in curbing this growing menace. It outlines relevant laws, including the Information Technology Act, 2000, and the Indian Penal Code, 1860, while highlighting gaps and challenges in enforcement and victim support.⁷

6. A Systematic Literature Review on Cyberstalking: An Analysis of Past Achievements and Future Promises

This systematic review synthesizes a decade of empirical knowledge on cyberstalking, analysing fifty studies to summarize existing knowledge. It identifies research themes on characteristics and roles of cyberstalkers, victims, parents, social media, and online service providers, providing a comprehensive overview of the field.⁸

7. Cyberbullying and Cyberstalking: Belongings and Anticipation Measures in India

This article delves into the effects of cyberbullying and cyberstalking in India, emphasizing their far-reaching and potentially life-altering consequences. It discusses anticipation measures and the importance of creating awareness to combat these issues effectively.⁹

8. Cyberbullying Amongst Teenagers in India: Addressing the Issue with the Information Technology Act of 2000

This blog post examines the role of the Information Technology Act of 2000 in addressing cyberbullying among Indian teenagers. It discusses the Act's effectiveness

and limitations in the evolving digital landscape, highlighting the need for updated legal provisions.¹⁰

9. The Phenomena of Cyber Bullying and Cyber Stalking

This paper examines the twin menace of cyberbullying and cyberstalking from both national and international perspectives. It analyzes why remedial action, especially in India, is slow and insignificant, and discusses present legal responses and the imperative to take urgent measures to counter these issues.¹¹

10. The Legal Landscape of Cyberbullying and Social Media Privacy

This article examines various legal provisions, policies, and guidelines in the Indian legal system regarding child protection and social media privacy. It highlights world-class standards and efforts taken by the government and corporate companies to address cyberbullying, culminating in practical recommendations for improvement.¹²

a. Statement of the Problem

Ironically, social media, which was first created to promote connection and communication, has turned into a tool for damage, especially in the form of cyberstalking and cyberbullying. Although social media sites like Instagram, Facebook, Twitter, and Snapchat give users a place to express themselves and connect with others, they also put people—particularly women and teenagers—at risk for identity theft, psychological suffering, and targeted abuse. Because social media is global and sometimes anonymous, it is challenging for forensic investigators and law enforcement to find offenders and bring about justice. There is still a big gap in the overall approach to dealing with these digital crimes, even with laws like the Indian Penal Code and the Information Technology Act of 2000. This problem is made worse by the proliferation of advanced technologies, phoney accounts, and encrypted conversations. In order to determine how well-equipped current laws, digital forensics, and platform rules are to combat cyberbullying and cyberstalking in the digital era, the research will critically examine how social media has turned into a double-edged sword.

b. Research Question

1. In what ways do social media sites' designs encourage cyberstalking and cyberbullying?
2. What effects do these crimes have on victims on a social, legal, and psychological level?
3. How well do India's present forensic procedures and legal frameworks handle these online crimes?

4. From the standpoint of victim protection and law enforcement, what are the shortcomings and restrictions in the existing system?
5. What technology advancements or changes may improve the forensic and legal response to these problems?

c. Objective of the Study

- To examine how social media contributes to the spread of cyberstalking and cyberbullying.
- To investigate pertinent Indian legal precedents and legal frameworks pertaining to internet harassment.
- To use case studies and empirical research to comprehend the psychological and emotional impacts on victims.
- To evaluate the effectiveness of forensic methods applied in situations of stalking and cyberbullying investigation and prosecution.
- To suggest institutional, technical, and legal changes aimed at reducing these cybercrimes.

d. Research Methodology

A qualitative and doctrinal research technique is used in this study, with a little amount of empirical data from case reports and secondary victim testimonials. These techniques are employed:

- **Doctrinal research:** Examining applicable international treaties and laws including the POCSO Act, the Indian Penal Code, and the Information Technology Act of 2000.
- **Analysis of significant Indian and foreign cases:** (such as the Amanda Todd case, the BOIS Locker Room case, and the Bulli Bai case) is how case studies are conducted. Secondary data analysis: includes news media, government white papers, academic articles, NCRB reports, and data from cybercrime helplines.
- **Comparative analysis:** Reviewing other nations' legal frameworks and digital safety regulations (such those in the UK, USA, and EU) for best practices is known as comparative analysis.

1.5 Scope of the Study

While making parallels from a few other countries, this study focusses on India. It examines

how social behaviour, technology, and the law interact, particularly as it relates to cyberbullying and cyberstalking on social media. The research is limited to: Commonplace social media platforms enhance online behaviours. Indian forensic skills and legal answers. cybercrimes that target people, particularly women, children, and users who are more susceptible. It leaves out more general categories such as state-sponsored cyber operations, hacktivism, and financial cybercrimes.

1.6 Hypothesis

The features and structure of social media platforms significantly contribute to the facilitation and proliferation of cyberbullying and cyberstalking, and current legal and forensic responses in India are inadequate in addressing these crimes effectively.

CHAPTER II **THE DIGITAL TERRAIN OF HARASSMENT UNDERSTANDING** **CYBERBULLYING AND CYBERSTALKING**

2.1 Detailed Definitions and Typologies of Cyberbullying and Cyberstalking

Cyberbullying and cyberstalking represent two pervasive and deeply harmful forms of digital harassment, often enabled by the accessibility and features of social media platforms.¹³ Though related, these terms cover distinct behavioural patterns with unique legal and psychological implications.

Cyberbullying refers to deliberate, repeated, and hostile behaviour by an individual or group intended to harm another person through digital mediums. This can manifest through online threats, spreading of false rumours, sharing of private or embarrassing images, exclusion from online groups, and mocking through memes or comments. Cyberbullying often occurs among peers especially schoolchildren and adolescents and frequently overlaps with offline bullying.¹⁴

Cyberstalking, on the other hand, is more calculated, persistent, and predatory in nature. It involves a pattern of behaviour where an individual uses electronic communication to monitor, threaten, or intimidate another person. Common forms include sending repeated unwanted messages, tracking a person's online activities, impersonation, or even doxxing publishing personal information such as addresses or phone numbers. Cyberstalking is often gendered, with women disproportionately affected, and it frequently intersects with intimate partner violence and obsessive behaviour.¹⁵

Several typologies exist within these two broad categories. In **cyberbullying**, researchers have classified behaviours into types such as flaming (online fights), harassment (repetitive offensive messages), denigration (spreading false rumours), impersonation (hacking or pretending to be someone), outing (sharing secrets or embarrassing information), exclusion, and cyber threats. In **cyberstalking**, the typology may involve surveillance-based stalking, identity fraud, and proxy stalking where the perpetrator enlists others to harass the victim. The digital environment intensifies the harm caused by these actions. Unlike traditional bullying or stalking, the virtual world offers no refuge for the victim. Content can go viral, remain online permanently, and reach a vast, sometimes global, audience. The aggressors often operate behind fake identities or anonymous accounts, emboldened by the illusion of invincibility and the lack of immediate consequences. Both cyberbullying and cyberstalking blur the line between online and offline harm, leading to real-world emotional, social, and sometimes legal ramifications. Their recognition as distinct cybercrimes is essential to formulating appropriate legal responses and forensic investigative procedures. Understanding their typologies helps in early identification, risk assessment, and victim support interventions, laying the foundation for responsive legal and digital safety frameworks.

2.2 How Social Media Facilitates: Anonymity

One of the most defining features of the internet particularly social media is the possibility of **anonymity**. This element of digital interaction plays a pivotal role in enabling and exacerbating cyberbullying and cyberstalking. While anonymity may protect privacy and freedom of expression in authoritarian regimes or sensitive discussions, in the context of online abuse, it serves as a dangerous enabler of harassment.¹⁶ Social media platforms allow users to create accounts with little to no verification of identity. This results in an environment where individuals can hide behind false names, generic profile pictures, and fabricated information. Anonymity, in such cases, provides a psychological shield that emboldens users to behave in ways they might never dare to in person.¹⁷ It eliminates the fear of social or legal consequences, encouraging more aggressive, abusive, or predatory behaviour. In the context of **cyberbullying**, anonymity allows perpetrators to launch attacks without fear of identification. Troll accounts or “burner” profiles are commonly used to harass individuals through hate speech, body shaming, slurs, and targeted humiliation. Victims often remain unaware of the identity of their abusers, leaving them confused, fearful, and psychologically vulnerable. This ambiguity can amplify the trauma, as the victim constantly wonders whether the attacker is someone known in real life.

Cyberstalking, similarly, thrives in an anonymous or pseudonymous environment. Stalkers may create fake accounts to monitor the victim's digital activities, interact with their friends and family, or send threatening messages without being detected. The use of proxy servers, VPNs, and disposable emails further allows stalkers to mask their digital footprints. In many cases, victims report a sense of being watched but cannot gather evidence or confirm who is behind the stalking. This psychological terror can lead to a state of constant anxiety, hypervigilance, and even social withdrawal.

Additionally, platforms that promote anonymity such as Reddit, 4chan, or anonymous question apps like Sarahah and ASKfm have seen a higher prevalence of cyberbullying. While these forums can offer safe spaces for open dialogue, they also create loopholes that abusers exploit. From a forensic perspective, anonymity poses a significant barrier to investigation and prosecution. Tracing IP addresses, decrypting communications, and linking accounts to real identities often requires cooperation from international service providers and complex digital expertise. This complicates timely legal action, allowing perpetrators to continue abusing their victims with impunity. Therefore, while anonymity can be a shield for free speech, it has, in the context of cybercrime, become a sword used against the vulnerable. Striking a balance between privacy rights and accountability is thus a critical challenge in regulating social media and combating online abuse.

2.3. How Social Media Facilitates: Amplification of Harm

One of the most dangerous aspects of cyberbullying and cyberstalking is the **amplification of harm** that social media inherently facilitates. Unlike traditional forms of bullying or stalking, the digital environment transforms what might have once been private or localized incidents into public spectacles with potentially global reach and long-lasting consequences. Social media platforms are designed for **virality** through likes, shares, retweets, reposts, and algorithms that promote engagement.¹⁸ While this architecture supports visibility for positive content, it also enables the rapid spread of harmful messages, images, or videos. When a victim is targeted through online bullying, defamatory posts or doctored images can circulate quickly across various platforms, magnifying the scale of the humiliation. Even a single offensive post can snowball into a wave of hate, as users who don't know the victim personally join in the abuse. This amplification is also evident in the **persistence and permanence** of digital content.¹⁹ Once shared online, harmful material can be screenshotted, archived, or reshared endlessly, making it virtually impossible to fully erase. For victims, this means the trauma is not momentary; they may relive the abuse repeatedly. In the case of cyberstalking, this can

include threats or private images resurfacing over time, even years later, causing renewed distress and traumatization. Moreover, the **audience size** plays a crucial role in increasing the psychological damage. In real-life bullying, a victim might face harassment from a limited peer group. Online, the potential audience is limitless.²⁰ When bullying or stalking is witnessed by thousands sometimes millions of people, the impact on the victim's dignity, self-esteem, and mental health can be devastating. This digital "mob mentality" also dilutes individual accountability, making it harder to identify and punish each perpetrator. A significant challenge is posed by **platform algorithms** that often fail to distinguish harmful content from popular content.²¹ Abusive posts may trend, not because they are appropriate, but because they generate high engagement through outrage, shock, or hate. This further incentivizes online bullies and stalkers who seek validation, attention, or power. Furthermore, **group targeting** becomes easier with social media's infrastructure. Victims can be added to abusive group chats, tagged in humiliating posts, or mass reported to suppress their voice. This enables coordinated attacks that intensify the psychological toll. Thus, the structure and culture of social media amplify not only the frequency of cyber harassment but also its depth and consequences. Without stringent content moderation, robust reporting mechanisms, and algorithmic reform, social media will continue to act as an accelerant for digital abuse.

2.4. How Social Media Facilitates: Untraceable Threats

One of the most sinister aspects of cyberbullying and cyberstalking in the digital age is the ease with which perpetrators can issue **untraceable threats**.²² Social media platforms, while designed to foster connection and expression, inadvertently create environments where anonymous or pseudonymous users can intimidate, threaten, and harass others without leaving an identifiable trail. This ability to inflict harm without fear of being caught significantly emboldens online abusers. The untrace ability of threats stems largely from the **technical affordances of the internet**. Cyberstalks and bullies often employ fake accounts commonly referred to as "sock puppet" or "burner" accounts which are created using temporary emails or phone numbers and often linked to no real identity. These accounts can be deactivated instantly after a threat is made, thereby wiping the surface-level evidence. In more advanced cases, perpetrators use **Virtual Private Networks (VPNs)**, proxy servers, and encryption tools to obscure their IP addresses and digital footprints, making it difficult for law enforcement or forensic teams to trace the source of the attack.²³ In India and other developing nations, this problem is further compounded by the **lack of mandatory KYC (Know Your Customer)** norms for social media accounts. Unlike financial institutions, most platforms do not require

users to verify their identity. Although some Indian laws such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, mandate due diligence by intermediaries, enforcement remains weak and inconsistent.²⁴ These **untraceable threats** often include rape threats, death threats, blackmail, or doxxing warnings (threats to publish private information), and disproportionately target women, minors, journalists, and activists. In many cases, the fear caused by the inability to identify the sender results in extreme emotional distress, sleep disturbances, and even withdrawal from public life. Victims often hesitate to report due to the belief that the threat cannot be tracked or that authorities will not take it seriously. From a forensic perspective, while it is possible to trace threats through device forensics, server logs, and metadata analysis, the process is time-consuming and requires cooperation from tech companies, which may be located in foreign jurisdictions. Moreover, many local police forces lack the digital literacy and technical resources to pursue such investigations effectively. Therefore, untraceable threats remain one of the most formidable challenges in tackling cyber harassment. Legal reforms requiring identity verification, better training of cyber cells, and international cooperation are crucial to addressing this invisible but deeply damaging facet of online abuse.

2.5 Victim Profiles: Children, Women, LGBTQ+ Individuals, Influencers

Cyberbullying and cyberstalking are not indiscriminate crimes they often target specific demographics more than others. The architecture of social media platforms, combined with existing societal biases, disproportionately impacts children, women, LGBTQ+ individuals, and public figures like influencers.²⁵ Understanding these victim profiles is crucial to crafting targeted legal and psychological support systems. Children and Adolescents are among the most vulnerable online users. As digital natives, they spend significant time on platforms like Instagram, Snapchat, and gaming chatrooms, often unsupervised. Cyberbullying among peers through name-calling, exclusion, spreading false rumours, and non-consensual image sharing is rampant. Children may not always comprehend the long-term implications of online harm or feel safe enough to report it. In severe cases, bullying has driven minors to depression, self-harm, and suicide. Additionally, online predators often exploit children's naivety through grooming, making this demographic doubly vulnerable to both bullying and stalking. Women face a highly gendered form of digital abuse, which includes image-based sexual abuse, slut-shaming, rape threats, and misogynistic trolling. Studies globally, including in India, show that women journalists, activists, and independent creators receive a disproportionate volume of online abuse. Stalkers often target women through persistent DMs, non-consensual tracking,

and publishing private information (doxxing).²⁶ The fear of being watched, judged, or harmed in real life due to online activity deeply affects women's mental health and limits their digital participation.

LGBTQ+ Individuals are also frequently targeted online due to prevailing prejudices, especially in conservative societies.²⁷ Queer individuals face cyberbullying in the form of outing (revealing someone's sexual orientation without consent), homophobic slurs, exclusion from digital communities, and threats of violence. Social media can be a double-edged sword for this community it offers a space for expression but also exposes them to heightened scrutiny, especially if their identity is not yet public or accepted in their personal circles. Influencers and Public Figures due to their visibility often attract massive online attention, not all of it positive. While many use social media as their career platform, they face a constant barrage of trolling, body-shaming, hate campaigns, and obsessive fan behaviour that often escalates into stalking. The psychological toll is immense, with many influencers reporting burnout, anxiety, and even stepping away from social platforms for self-preservation. Despite their differing vulnerabilities, all these groups suffer from inadequate legal protection and support mechanisms. Many choose silence over confrontation due to fear, stigma, or lack of trust in legal redress. Thus, victim-specific digital safety policies, legal reforms, and mental health support are necessary to protect these individuals from cyber harassment.

2.6. Psychological and Emotional Consequences: Depression, Anxiety, Suicide

The psychological and emotional consequences of cyberbullying and cyberstalking are profound and far-reaching. Unlike physical forms of harassment that may have visible signs, the emotional scars inflicted by digital abuse are often invisible, internalized, and long-lasting. Victims frequently report a sense of helplessness, isolation, and severe mental health deterioration that can culminate in depression, anxiety disorders, and, tragically, even suicide. One of the primary psychological impacts of online harassment is **depression**.²⁸ Victims of persistent cyberbullying or stalking often experience prolonged sadness, loss of interest in daily activities, and feelings of worthlessness. These emotions are not merely fleeting reactions; they develop as a result of repeated exposure to hostility, humiliation, and the inability to escape the abuse. Since social media is now embedded into daily routines, logging off becomes increasingly difficult, trapping victims in a cycle of victimization. **Anxiety disorders** are another common outcome. Victims often describe a constant state of fear and unease, not knowing when or how the next attack will come.²⁹ This can evolve into chronic anxiety or panic attacks, particularly when the abuse includes threats of physical harm or doxxing. In

cases of cyberstalking, the victim might suffer from hypervigilance constantly looking over their shoulder or obsessively checking online mentions and messages. The fear of being watched or followed, even virtually, is deeply destabilizing.

Perhaps the most devastating consequence is the link between online abuse and **suicidal ideation** or completed suicide. Numerous global cases have highlighted this tragic progression. In India, the suicide of a 14-year-old girl in 2020 due to cyberbullying on TikTok brought national attention to the issue. Similarly, high-profile international cases like that of Amanda Todd in Canada or Megan Meier in the U.S. underline how severe and unrelenting online abuse can push vulnerable individuals, especially adolescents, to end their lives. The emotional weight of being constantly ridiculed, threatened, or exposed online becomes unbearable when victims feel that no escape or support system exists. Furthermore, **secondary trauma** experienced by family members, close friends, or even bystanders is a lesser discussed but significant consequence. Witnessing a loved one spiral due to online abuse can lead to shared anxiety and depression among the victim's immediate circle. Despite the scale of the issue, access to **psychological support** remains limited. Many victims do not seek therapy due to stigma, financial barriers, or unawareness. This calls for urgent investment in digital mental health services, school and workplace-based support systems, and sensitization campaigns that promote psychological resilience and early intervention.

CHAPTER III:

LEGAL AND FORENSIC FRAMEWORK IN INDIA

3.1. Relevant Indian Laws

a. **Information Technology Act, 2000**

The **Information Technology Act, 2000** (IT Act) is a crucial legal instrument in India for regulating cyber activities, including the digital perpetration of cyberbullying and cyberstalking.³⁰ The Act's core objective is to promote e-commerce and secure electronic transactions, but it also provides the legal foundation for addressing digital offenses.

- **Section 66E** of the IT Act specifically addresses the violation of privacy by criminalizing the capturing, publishing, or transmitting of images of a person's private area without consent. This provision is particularly pertinent in cases of image-based sexual abuse and cyberbullying, where personal photographs or videos are shared without permission to harass or shame the victim.

- **Section 67** deals with the publication and transmission of obscene material in electronic form, criminalizing the distribution of explicit content that may be used in online bullying or defamation campaigns. This is crucial in cases where cyberbullies share pornographic material to demean or intimidate their victims.
- **Section 67A** extends this by criminalizing the transmission of sexually explicit content involving minors, addressing online sexual exploitation.
- **Section 67B** targets child sexual abuse material (CSAM) specifically, addressing online grooming and exploitation of minors, which is central to cases involving cyberstalking and exploitation through social media platforms.

While the IT Act provides a legal framework, its application in cases of cyberbullying and cyberstalking often encounters challenges.³¹ The definitions of cyberstalking and cyberbullying are not always clearly outlined, leading to inconsistent enforcement.

Furthermore, the Act does not sufficiently address emerging forms of digital abuse such as online harassment through fake identities or deepfake technology.

b. Indian Penal Code (IPC), 1860

The **Indian Penal Code (IPC)** offers several provisions that are relevant for addressing cyberbullying and cyberstalking, which often have an emotional and psychological toll on the victim. These provisions help bridge the gap in the IT Act by offering traditional criminal protections that are applicable to digital contexts.

- **Section 354D** of the IPC criminalizes cyberstalking, explicitly penalizing repeated online contacts or monitoring of a person's activities without consent, with a specific focus on women. This provision is a critical tool for tackling cases where individuals face persistent harassment through social media, such as continuous unsolicited messages, threats, or demands for attention.
- **Section 507** is pertinent when harassment or intimidation occurs through anonymous communication. It criminalizes threatening communications made in a way that prevents the identification of the perpetrator. This section is especially important in cyberstalking cases where threats are made without revealing the stalker's identity, often through burner accounts or anonymous messaging platforms.
- **Sections 499 and 500** relate to defamation, which is often a significant element in cyberbullying. Online defamation, where a person's reputation is tarnished through false information or harmful statements, can have severe consequences for victims,

leading to mental health issues, social ostracization, and reputational damage.

Despite the IPC's provisions, challenges in the enforcement of cyberstalking and defamation laws arise due to difficulties in tracking perpetrators, especially when they operate under the veil of anonymity.

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

The **POCSO Act, 2012**, was introduced to provide a comprehensive legal framework for protecting children from sexual offenses, including digital crimes. The act criminalizes various forms of child sexual abuse, including online exploitation, grooming, and the sharing of exploitative material.

- **Section 11** of the POCSO Act addresses offenses such as child pornography, online grooming, and any act that involves the exploitation or abuse of a minor through digital media. Cyberstalks targeting children may use social media to engage in grooming behaviour, where they build a relationship of trust with the child to manipulate or exploit them.
- **Section 13** of the POCSO Act criminalizes the use of children for the creation, transmission, or circulation of child sexual abuse material. This section is particularly relevant when cybercriminals use platforms like social media to disseminate such content.

The expansion of the POCSO Act in 2019, which introduced provisions for stricter punishments related to online child sexual abuse material, reflects the growing recognition of the internet's role in facilitating such crimes.³² However, challenges remain, particularly regarding the identification of perpetrators and cross-border legal enforcement. The act provides important protections but also highlights the limitations in preventing online exploitation, especially in cases where the abuse occurs on social media platforms without the victim's awareness.

3.2. **Judicial Precedents**

Indian judicial precedents play a significant role in shaping the interpretation and application of laws related to cyberbullying and cyberstalking. Courts have increasingly acknowledged the need for a more robust legal framework to address online harassment and digital abuse, particularly through landmark judgments.³³

- **K.S. Puttaswamy v. Union of India** (2017)³⁴ was a landmark case where the Supreme

Court of India upheld the **right to privacy** as a fundamental right under the Indian Constitution. This ruling has been instrumental in advocating for stricter privacy protections for individuals in the digital space, including cases of cyberbullying and online harassment. The judgment strengthens the argument for enhanced privacy laws on social media platforms and establishes a legal foundation to fight digital violations.

- **Shreya Singhal v. Union of India** (2015)³⁵ is another pivotal case where the Supreme Court struck down **Section 66A** of the IT Act, which criminalized the sending of offensive messages through communication service, websites, or applications. The court ruled that the section was overly vague and violated the fundamental right to freedom of speech and expression. This judgment, while protecting free speech, also highlighted the gap in laws addressing online abuse and the need for clearer and more specific provisions for cyberbullying.
 - In the **State v. S. Harish** (2024)³⁶ case, the courts reinforced the application of the **IT Act and POCSO Act** in cases of online child exploitation and harassment. This case marked a significant shift in how courts address digital abuse involving minors, emphasizing the role of social media platforms in facilitating harmful activities and underlining the necessity of stronger regulatory measures.
- These precedents indicate an evolving understanding of cybercrime in India. However, they also underscore the need for more nuanced legislation that can address the diverse and dynamic nature of cyberbullying and cyberstalking.

3.3. Digital Forensic Investigation Tools

Digital forensics plays a crucial role in investigating cybercrimes, including cyberbullying and cyberstalking. These tools enable forensic experts to extract, preserve, and analyse digital evidence in a way that is admissible in court.³⁷

- **Autopsy** is an open-source digital forensics tool that is widely used by law enforcement agencies. It helps recover files, logs, and browser histories from devices, making it a valuable tool in cases of cyberstalking or cyberbullying. For instance, Autopsy can retrieve deleted conversations or images that may be crucial in identifying the perpetrator of online harassment.
- **FTK (Forensic Toolkit)** is another popular digital forensics tool used to analyse email accounts, files, and communications. It provides a user-friendly interface and powerful indexing features that help in recovering and searching for critical evidence. In

cyberstalking cases, FTK can be used to analyse large volumes of data from messaging apps, emails, and social media platforms to track harassing patterns.

- **Cellebrite** is a mobile forensics tool that specializes in extracting data from smartphones. Given the increasing use of mobile devices for cyberbullying, Cellebrite can help forensic investigators analyse communication apps, social media profiles, and multimedia files stored on the victim's or perpetrator's device. This tool is essential in cases where harassment occurs via private messages, social media platforms, or even encrypted communications.
- **EnCase** is a comprehensive digital forensics suite used for the analysis of computers, mobile devices, and networks. It is known for its detailed reporting features and its ability to handle large volumes of data. EnCase is highly regarded in the law enforcement community for its role in investigating complex cybercrimes and gathering evidence that can withstand legal scrutiny.

These tools are vital in ensuring that evidence is properly collected and preserved for successful prosecution. However, their effectiveness depends on the availability of training, resources, and timely action by investigators.

3.4. Challenges in Evidence Collection, Jurisdiction, and Data Retrieval

While digital forensic tools have made great strides in cybercrime investigation, several challenges persist in evidence collection, jurisdiction, and data retrieval that hinder effective legal proceedings in cyberbullying and cyberstalking cases.³⁸

- **Evidence Volatility:** Social media content is inherently volatile. Online abuse is often perpetrated in the form of direct messages, posts, or videos that can be deleted within moments of being posted. The speed at which information is removed or altered presents a significant challenge for forensic investigators, who must act quickly to preserve evidence. This volatility requires forensic experts to employ real-time data capture techniques to mitigate the risk of losing critical evidence.
- **Jurisdictional Issues:** Cybercrimes, particularly those committed across borders, present significant jurisdictional challenges. Social media platforms, where the majority of cyberbullying and cyberstalking occurs, often operate under global frameworks with servers located in different countries. This makes it difficult for Indian law enforcement agencies to access data unless the companies cooperate with Indian authorities. International treaties like **Mutual Legal Assistance Treaties (MLATs)** are

essential but often slow and inefficient.

- **Data Retrieval from Encrypted Sources:** Many cybercriminals use encryption tools, such as VPNs, proxies, and end-to-end encrypted messaging apps (e.g., WhatsApp, Signal), to conceal their identities and activities. Retrieving data from these encrypted sources presents a significant hurdle, as it requires legal permissions and technical expertise.
- **Lack of Training and Resources:** Digital forensics remains a highly specialized field, and many police departments in India lack the necessary infrastructure and trained personnel to handle complex cybercrime cases. Forensic investigations often face delays due to a lack of resources or expertise, further impeding the timely resolution of cases.

3.5. Role of Cyber Cells and Digital Forensic Units

Cyber Cells and Digital Forensic Units in India play a pivotal role in addressing the rising tide of cyberbullying and cyberstalking. These specialized units are tasked with investigating digital crimes and providing forensic support to ensure that perpetrators are held accountable.³⁹

- The **Indian Cyber Crime Coordination Centre (I4C)**, established by the Ministry of Home Affairs (MHA), is a critical initiative aimed at combating cybercrime in India. It provides a central framework for investigating cybercrimes, including cyberbullying, and coordinating efforts across states. Through this initiative, a **national cybercrime reporting portal** (cybercrime.gov.in) was created, enabling citizens to report cybercrimes and online harassment anonymously.
- State police departments have also established their own **Cyber Crime Cells** to handle the increasing number of complaints related to online abuse, cyberstalking, and harassment. These units are responsible for providing a swift response to victims, conducting digital forensic investigations, and collaborating with other law enforcement agencies.
- In addition, **Digital Forensic Units** are being increasingly established within state police departments to specialize in recovering, analysing, and preserving digital evidence in cybercrime investigations. These units use advanced forensic tools like FTK, EnCase, and Cellebrite to track perpetrators, recover deleted content, and identify evidence crucial to prosecution.

Despite the efforts of these units, there is still a significant gap in terms of nationwide coverage,

training, and technology. The implementation of a more cohesive national strategy and improved infrastructure for cybercrime investigation is essential to effectively combat the growing menace of cyberbullying and cyberstalking in India.

CHAPTER IV:

PLATFORM RESPONSIBILITY AND COMPARATIVE ANALYSIS

.1. Role of Platforms: Facebook, Instagram, Snapchat, Twitter/X, YouTube

Social media platforms play a crucial role in shaping online interactions, and their influence extends far beyond simply providing spaces for connection and communication. Platforms like **Facebook, Instagram, Snapchat, Twitter/X, and YouTube** have become powerful tools for both positive engagement and harmful behaviours, including **cyberbullying** and **cyberstalking**.⁴⁰

- **Facebook:** As one of the largest social networking sites globally, Facebook facilitates interactions among millions of users, both public and private. While it has introduced features like content reporting, comment filtering, and anti-harassment policies, the platform continues to face challenges in preventing and responding to online abuse. The sheer volume of content posted daily on Facebook makes real-time moderation difficult, and abusive posts often go unnoticed or unaddressed for extended periods. Moreover, Facebook's automated systems sometimes fail to accurately identify subtle forms of cyberbullying, such as indirect threats or trolling disguised as humour.
- **Instagram:** Owned by Meta, Instagram is a visual platform that allows users to share photos and videos. Unfortunately, its visual nature contributes to the prevalence of body-shaming, harassment based on appearance, and the spreading of inappropriate or harmful content. Instagram has implemented a range of safety features, including comment controls, message filters, and reporting mechanisms for abusive posts. However, Instagram remains a fertile ground for cyberbullying, particularly for teenagers and influencers who are targeted for their appearance, behaviour, or opinions.
- **Snapchat:** Snapchat has a unique feature **disappearing messages** that can exacerbate the problem of cyberbullying and cyberstalking. The temporary nature of messages encourages users to share abusive content without fear of long-term consequences. This ephemeral feature also complicates the task of collecting evidence, leaving victims vulnerable and without recourse. Furthermore, Snapchat's private nature often shelters perpetrators from immediate accountability.

- **Twitter/X:** Twitter has long been known for fostering heated debates, and its algorithms tend to prioritize controversial and often harmful content. This has led to widespread cyberbullying, particularly against high-profile figures, marginalized groups, and activists. Despite Twitter's efforts to introduce anti-harassment policies, the platform struggles with managing abusive accounts, often allowing perpetrators to remain active for long periods, especially when the victims are not prominent figures.
- **YouTube:** YouTube has millions of active users and offers a platform for video content creation, discussion, and interaction. However, its comment sections often become hotbeds for harassment and defamation. The inability of YouTube's moderation tools to consistently address comments that may promote hate speech, harassment, or bullying leaves many users exposed to malicious online behaviours.

Each platform, despite implementing various tools and guidelines to tackle harassment, continues to grapple with the prevalence of cyberbullying and cyberstalking. The challenge lies in balancing user freedom with the need for protecting vulnerable individuals from harm.

.1. Analysis of Content Moderation Policies and Transparency Reports

Content moderation is one of the most critical aspects of combating cyberbullying and cyberstalking on social media platforms. Social media companies are tasked with creating a balance between freedom of expression and protecting users from harm. However, the transparency and effectiveness of these content moderation policies are often questioned.⁴¹

- **Facebook and Instagram:** Meta, the parent company of Facebook and Instagram, uses a combination of **automated tools** (AI) and **human moderators** to monitor content. These tools can detect abusive language, hate speech, and threats in posts, comments, and direct messages. Users can also report harmful content, which is reviewed by human moderators. However, the scope of Facebook's moderation is limited, and the platform's vast scale makes it difficult to act on every report in a timely manner. Moreover, Facebook's algorithm is designed to prioritize engagement, which often leads to controversial or abusive content being amplified and spread more rapidly. Facebook has introduced more robust features over time, including **comment controls** and **keyword filtering**, but issues like **harassment in private groups** and **targeting individuals through memes** continue to persist. Transparency reports, while offering insights into the volume of removed content, fail to provide clarity on the effectiveness of these policies in preventing abuse.⁴²

- **YouTube:** YouTube's content moderation system is designed to remove harmful videos, comments, and live streams that violate its **community guidelines**. However, with millions of videos uploaded daily, it's not always feasible for YouTube to spot and remove harmful content quickly. In the past, YouTube has faced significant backlash for allowing hate speech, cyberbullying, and harmful content to remain on the platform for extended periods. The platform's **automated systems** sometimes fail to accurately identify nuanced instances of harassment, leaving some abusive content visible for longer than it should be. YouTube's **transparency reports** have improved in recent years, but users often feel the platform is slow to act on harmful behavior, particularly in cases of **cyberstalking**.
 - **Twitter/X:** Twitter's **reporting system** allows users to flag abusive content, and the platform has introduced **safety tools**, such as **mute**, **block**, and **restrict** features. Despite this, Twitter struggles with **harassment**, especially for women, marginalized communities, and activists. Critics argue that Twitter's efforts are reactive rather than preventive, as abusive content often remains visible until it garners significant attention. **Transparency reports** by Twitter provide some insights into the platform's content moderation but fail to comprehensively address the systemic issues in combating harassment. In particular, Twitter has been criticized for allowing **trolls** to operate with minimal consequences.
 - **Snapchat:** Snapchat's content moderation is relatively less visible compared to other platforms, as most interactions occur through **private messaging** and **ephemeral posts**. Although the platform does provide reporting tools for users, the disappearing nature of content makes it more difficult for moderators to take action. **Transparency reports** are sparse, and Snapchat has been criticized for not doing enough to combat abuse, particularly when it comes to **cyberstalking**.
- The transparency and accountability of content moderation policies across these platforms are inconsistent. While all these platforms have mechanisms to report and remove harmful content, the **speed** and **effectiveness** of these processes vary. More robust and transparent reporting and moderation systems are needed to address the growing challenge of online abuse.

.1. How Tech Features Contribute to Abuse (e.g., Disappearing Messages, Encrypted DMs)

The very technology that makes social media platforms user-friendly and engaging also provides avenues for **cyberbullying** and **cyberstalking**. Some of the tech features designed to enhance user privacy and security inadvertently encourage or facilitate abusive behavior.

- **Disappearing Messages:** Platforms like **Snapchat** and **Instagram** popularized the use of disappearing messages, which are designed to enhance privacy by ensuring that messages are automatically deleted after being viewed. However, this feature has been misused by **cyberbullies** and **cyberstalkers**, who exploit the temporary nature of the messages to send harmful content without fear of leaving a lasting record. Since the messages disappear, victims often have no evidence to present when they report the harassment, making it more difficult to hold perpetrators accountable.

Additionally, disappearing messages can lead to **escalated harassment**, as the perpetrator may send repeated threats or abusive content without facing immediate consequences. This ephemeral nature creates a **sense of impunity** for abusers, as there is no lasting record of their behavior.⁴³

- **Encrypted Direct Messages (DMs):** **Encrypted messaging** services like **WhatsApp** and **Telegram** are often touted as a safe and secure way to communicate. While encryption ensures privacy and protects user data from unauthorized access, it also poses challenges for law enforcement and content moderators in cases of **cyberstalking**. Encrypted messages prevent anyone, including platform administrators, from accessing the contents of private messages, making it harder to detect and prevent abusive behaviors.

While encryption is valuable for protecting users from surveillance, it creates a **double-edged sword**. **Stalkers** can use encrypted platforms to target their victims without detection, and the victims may not even know who is behind the abuse. Additionally, it becomes harder for victims to **retain evidence** of harassment when the conversations are securely encrypted and stored only on the devices of the involved parties.

Platforms that offer disappearing messages or end-to-end encryption must find ways to balance user privacy with the need to protect individuals from harm. **Stronger regulatory frameworks** could require tech companies to implement better safeguards against abuse, including tools for recovering or reporting **deleted messages**.

.2. Accountability Gap: Safe Harbor Protection vs. User Safety

One of the most significant legal challenges in tackling online harassment is the **accountability gap** between platform responsibility and user safety. The concept of **Safe Harbor** protection, enshrined in laws like the **Information Technology Act, 2000** in India, shields platforms from liability for the actions of their users, provided they follow due diligence procedures.

- **Safe Harbor Protection:** Under this legal framework, social media platforms are treated as **intermediaries**, not the publishers of user-generated content. This means platforms are generally not held responsible for harmful content posted by users unless they actively moderate or intervene in such content. For example, if a user posts defamatory or abusive content, the platform is not liable for any harm caused, as long as they take appropriate action when the content is reported.

While this protection fosters a free and open internet, it also creates a loophole, as platforms may be incentivized to avoid taking responsibility for harmful content. Rather than proactively monitoring content or implementing safeguards against **cyberbullying** or **cyberstalking**, platforms may opt to implement minimal moderation policies and only act when explicitly prompted by user reports.⁴⁴

- **Accountability Gap:** The **accountability gap** is a critical issue when it comes to user safety. Since platforms are not held liable for user-generated content, they often prioritize **user engagement** over safety. This results in a **lack of preventive measures** against harmful content. **Cyberbullies** and **cyberstalkers** may exploit this legal loophole to target vulnerable individuals, knowing that the platforms will not face legal consequences for allowing the abuse to persist.

To address this gap, many have called for **stricter regulations** that hold platforms accountable for the safety of their users. This includes **greater oversight** of content moderation practices, **increased transparency**, and the implementation of **proactive measures** to prevent abuse. Some jurisdictions, like the **UK**, have begun implementing laws that demand greater accountability from platforms.

.3. Comparative Study

a. UK's Online Safety Bill

The UK's **Online Safety Bill** is a comprehensive piece of legislation designed to regulate online platforms, particularly in terms of user safety. It places a **duty of care** on social media companies, requiring them to take responsibility for harmful content on their platforms. This

includes the **proactive removal** of cyberbullying content and the creation of clear reporting systems for users to flag abusive material.

Platforms will be required to assess the risks of online harm and take steps to minimize them. The bill also includes penalties for companies that fail to comply with these obligations, making it one of the most **comprehensive digital safety laws**.

b. USA's Stop Cyberstalking Bill (Proposed)

The **Stop Cyberstalking Bill** in the United States aims to address the growing problem of **online harassment** and **cyberstalking**. It proposes **enhanced penalties** for those who use the internet to stalk, intimidate, or harass others. The bill emphasizes the importance of **law enforcement training** in handling cyberstalking cases and calls for the establishment of **specialized cyber units** to tackle such crimes.⁴⁵

The bill would allow victims to file lawsuits against perpetrators for cyberstalking, providing a legal pathway for seeking redress.

c. EU's Digital Services Act (DSA)

The **Digital Services Act (DSA)** of the European Union aims to regulate large online platforms by setting clear rules for **content moderation** and **user safety**. The DSA places responsibility on platforms to remove harmful content quickly and to ensure **transparency** in content removal processes. It also introduces specific protections for children and vulnerable individuals, requiring platforms to **adopt stronger measures** to prevent harm.⁴⁶

The DSA is expected to become a model for other countries, as it brings about greater accountability and transparency in content moderation.

.4. Best Practices and Lessons for India

India can draw valuable lessons from these international frameworks to improve its own approach to **cyberbullying** and **cyberstalking**.⁴⁷

By incorporating elements from the **Online Safety Bill** and **DSA**, India can **strengthen its legal framework** for user protection while ensuring that platforms take more responsibility for the safety of their users. Incorporating measures like **increased transparency** in content removal and **proactive monitoring** can enhance accountability.

At the same time, there is a need to balance **freedom of speech** with user safety, ensuring that platforms don't overreach in their moderation efforts while providing effective protection against harm.

4.7 The Definition and Scope of the Nature of CSEM

Any content pictures, films, or other that shows the sexual exploitation or abuse of kids is referred to as CSEM. In addition to being against the law, this content seriously harms the young victims. Coercion, manipulation, abuse, and child trafficking are frequently involved in the formation of CSEM. The people that produce, distribute, and use CSEM are a part of an international network that takes advantage of weaker children for financial gain or self-satisfaction.⁴⁸

As the internet has grown, so too has the problem's breadth. Criminal networks work internationally, sharing, selling, and consuming exploitative content via dark web forums, encrypted chat services, and social media sites. Because of this global aspect, it is challenging for authorities to find offenders and save victims.

4.8 Effects on the Victims

The repercussions on children who are sexually exploited are severe and persistent. Their anguish is not confined to the moment of abuse; it is frequently made worse by the ongoing dissemination of pictures or films showing their maltreatment.⁴⁹

The victims get even more traumatised each time they watch these materials because they know that many other people are also experiencing and sharing their misery. CSEM victims frequently encounter:

Psychological trauma: Victims of sexual abuse frequently experience depression, anxiety, PTSD, and thoughts of suicide.

Emotional distress: Even as adults, victims may continue to experience feelings of dread, humiliation, and guilt.

Social isolation: People who have been victimised may feel stigmatised and find it difficult to build relationships with others, as well as to trust others.

Lifelong vulnerability: People who have experienced child sexual abuse are frequently more likely to be exploited and abused in the future, both as children and as adults. These victims suffer not only personal but also societal harm since they find it difficult to reintegrate into society, which can have an impact on social services, healthcare systems, and communities.

4.9 Digital Technology's Role⁵⁰

The internet has changed society in many ways, but it has also served as a haven for child abuse. The creation, distribution, and consumption of CSEM have become simpler thanks to developments in digital technology. In the digital age, there are a number of causes that have

led to the rising issue of CSEM:

Anonymity: Criminals conceal their identities through the use of encryption, virtual private networks (VPNs), and anonymous internet forums, making it challenging for law authorities to find them.

Dark web: People can exchange and trade CSEM on encrypted networks without being readily discovered by conventional law enforcement techniques.

Social media and live streaming: By employing grooming strategies to win over trust, abusers can take advantage of minors via social media platforms.

Furthermore, live-streamed abuse often done for financial gain has emerged as a troubling trend that is more difficult to identify and stop.

Cloud storage: The use of cloud services makes it easier to store and distribute enormous amounts of exploitative content, which makes attempts to delete or limit access to CSEM more difficult.

Case Law

CASE LAWS Based on the CSEM⁵¹

IN THE HIGH COURT OF JUDICATURE AT MADRAS DATED: 11.01.2024

**THE HONOURABLE MR. JUSTICE N. ANAND VENKATESH CRL.O. P No.37 of 2024
And Crl.M.P No.79 of 2024 S.Harish S/o. Santhanam V.**

- 1. The Inspector of Police, AWPS – Ambattur, Chennai – 600 053.**
- 2. V. Ramani Inspector of Police, AWPS - Ambattur, Chennai - 600 053. Background**

The case centres on S. Harish, who was charged with downloading child-related pornography into his cell phone. A letter from the Additional Deputy Commissioner of Police (Crime against women and children) that underlined Harish's suspected role in obtaining such information served as the foundation for the prosecution's case.

It was indicated in the letter that the petitioner had downloaded child-related pornographic files on his mobile phone. After receiving the letter, the second respondent lodged a First Information Report in Crime No.03 of 2020 on January 29, 2020, for crimes under Sections 14(1) of the Protection of Children from Sexual crimes Act, 2012 and 67-B of the Information Technology Act, 2000.⁵²

Issues

This petition has been submitted on the Sessions Judge's file at Mahila Neethi Mandram (Fast Track Court), Tiruvallur District, with the intention of quashing the proceedings that are now

underway in Spl.SC. No.170 of 2023.

Legal proceedings

The Inspector of Police, the second respondent, filed a First Information Report (FIR) against Harish after obtaining the letter. Sections 67-B of the Information Technology Act of 2000 and Section 14(1) of the Protection of Children from Sexual Offences (POCSO) Act of 2012 were used in the framing of the accusations. Harish's cell phone was confiscated during the inquiry, and two files containing child pornography were found through forensic examination.

In these movies, young boys were shown having intercourse with an older lady or girl. A final report that was filed with the court was based on the evidence that was obtained.

Petitioner's Argument

In accordance with Section 482 of the Criminal Procedure Code (CrPC), Harish filed a Criminal Original Petition (CrI.O.P). He prayed that the Sessions Judge of Mahila Neethi Mandram (Fast Track Court), Tiruvallur District, would grant his request for access to the records in Special Sessions Case No. 170 of 2023, so that they might be quashed against him. The petitioner added that he is currently about 28 years old and that he was able to successfully break this habit over time. The petitioner was forthright enough to acknowledge that he could no longer support his addiction and that he would seek counselling in order to kick it.

Legal Analysis

A child or children must have been utilised for pornographic purposes in order for Section 14(1) of the Protection of Children from Sexual Offences Act, 2012 to establish an offence. This would imply that the accused party was responsible for the child's pornographic usage. Even in the unlikely event that the accused has seen child pornography, Section 14(1) of the Protection of Children from Sexual Offences Act, 2012, will not apply in this case. Given that he hasn't used a child or children for pornographic reasons, the accusation can only be seen as a moral decline on his behalf.

Section 67-B of the Information Technology Act, 2000 states that an accused individual must have published, transmitted, or generated content showing children engaging in sexually explicit acts or conduct in order for it to be considered an offence. According to a close reading of this clause, viewing child pornography does not in and of itself constitute a crime under Section 67-B of the Information Technology Act of 2000. Despite the broad wording of Section 67-B of the Information Technology Act of 2000, it does not apply in situations where an individual has downloaded child pornography onto an electronic device and has seen it without taking any further action.

The petitioner's cell phone was taken throughout the course of the inquiry and transferred to

the forensic science department for examination. The analyst provided a report that named two folders in particular that included child pornographic material. Boys (under the age of fifteen) were seen having sex with an adult lady or girl in those two films. Based on the documents obtained during the investigation, a final report was prepared and submitted to the lower court, where it was filed under Spl.SC. No.170 of 2023. Section 67-B of the Information Technology Act of 2000 and Section 14(1) of the Protection of Children from Sexual crimes Act of 2012 were the crimes for which the lower court granted cognisance.

On one occasion, the Kerala High Court addressed the application of Section 292 IPC. In one instance, a person was discovered to be watching pornographic movies, and a First Information Report was filed against him. In addressing this matter, the Kerala High Court ruled that a person's mere viewing of an offensive image or video does not automatically result in a violation of Section 292 IPC. This is because the individual in question does the act in private, unaffected by or influencing anybody else. The elements of the crime begin to work as soon as the accused attempts to distribute, disseminate, or display pornographic images or movies in public. Teenage porn addiction is a developing problem as a result of the ease with which one may get sexually explicit content on the internet. They can be exposed to many pages of pornographic content with just one click of a button. According to a recent survey, teens who use porn are as follows:

Before the age of 18, nine out of ten males are exposed to pornography in some capacity.

- Before turning 18, six out of ten girls are exposed to pornography.
- A guy often encounters pornography for the first time when he is 12 years old.
- 71% of teenagers have taken action to keep their parents from knowing what they do online.
- Boys between the ages of 12 and 17 are most susceptible to being addicted to porn.

Court decision

The Madras High Court ruled that viewing pornographic material privately after downloading it onto a computer does not violate Section 67-B of the Information Technology Act. Stated differently, downloading child pornography and not sharing it or distributing it further was not illegal under the mentioned statute. This decision resolved a conflict in the law by making it clear that private ownership of such content, provided it is not intended for distribution or sharing, will not result in criminal consequences. The court dismissed the case against S. Harish, stating that there was no criminal activity under the applicable laws while downloading child pornography for personal use.

Appeal in the Apex Court

The High Court of Judicature at Madras in criminal original petition the respondent no. 1 (accused) filed (Crl. O.P.) No. 37 of 2024 ("Impugned Order") under Section 482 of the Code of Criminal Procedure, 1973 (also known as the "Crpc"). The High Court granted the petition, quashing the chargesheet dated September 19, 2023, for offences punishable under Section 67B of the Information Technology Act, 2000 (also known as the "IT Act") and Section 15(1) of the Protection of Children from Sexual Offences Act, 20

12 (also known as the "POCSO"). The offences stemmed from the FIR No. 03 of 2020, P.S. Ambattur, Chennai. Consequently, Special Sessions Case No. 170 of 2023's criminal procedures were closed.

"Just Rights for Children Alliance," is a NGOs that collaborate to combat child trafficking, sexual exploitation, and related issues. On the other hand, one of the partner NGOs in the aforementioned collation, appellant no. 2, is a child rights organisation that works to protect children from exploitation.

Considering the grave public concern raised by the case, they requested permission from this Court to contest the High Court's contested decision. The State of Tamil Nadu and the Inspector of Police from the All-Women's Police Station in Ambattur, Chennai, are the second and third responder numbers, respectively.

Report of Forensic

- a) More than 100 pornographic video files were discovered to have been downloaded and stored on various pathways; further information on these videos may be obtained in Annexure II.
- b) Some of the pornographic video files were discovered to be kept.
- c) Two video files that may contain child pornography were discovered saved under the same directory. Boys (under the age of fifteen) were shown having intercourse with an adult lady or girl in the films.

Issues Examined

- I. What does the POCSO's Section 15 cover? Put otherwise, what is the fundamental difference between POCSO sub-sections (1), (2), and (3), respectively?
- II. Is it illegal under the POCSO to merely watch, possess, or save any child pornographic material?
- III. What is the real reach of IT Act Section 67B?

- IV. What does Section 30 of the POCSO cover? Put otherwise, whatever fundamental circumstances must be present in order to invoke the statutory presumption of guilty mental state with regard to Section 15 of the POCSO?
- V. Is it possible for the Special Court constituted under the POCSO to invoke the statutory presumption included in Section 30 of the POCSO just during the trial stage?

Relevant provision Protection of children from sexual

Section 2(1) (da): "Child pornography refers to any visual representation of sexually explicit behaviour involving children, including images produced by digital or computer technology that are indistinguishable from real children and images that have been altered or modified but still seem to show children;"

Section 15: POCSO defines when it is illegal to store or possess pornographic material involving children and specifies the associated penalties. It also specifies when such behaviour is unlawful.

Section 30: "Culpable mental state" encompasses purpose, motivation, factual knowledge, and the conviction or rationale for a factual belief.

Relevant provision Information Technology Act 2000

Section 67: is the principal provision that criminalizes the publication or transmission of "obscene material" in any electronic form and constitutes an offence.

Section 67 A: is a more aggravated offence, prescribing enhanced punishment than the preceding provision. It does so by further amplifying the scope of 'obscene material' by stipulating that any obscene material that contains or depicts any sexually explicit act or conduct, when published or transmitted shall be punishable under the said provision.

Section 67 B: specifically deals with child pornographic materials. It provides for an even more severe form of offence by bringing within its ambit those obscene materials in any electronic form that depict a child in any sexually explicit act or conduct and by further expanding the scope of 'actus reus' which is punishable under the provision to include not just publication or transmission but also the browsing, creation, collection, online facilitation or enticement of children into any sexual act or conduct etc

Precedents referred

- Similar to this, in **Akash Vijay v. State of Kerala**, reported in 2024 KER 42626, the Kerala High Court held that, absent evidence demonstrating that the accused individual

either purposefully downloaded or browsed the in-question material, or that he shared or transmitted it, the mere storage or possession of any pornographic material involving a child will not constitute an offence under Section(s) 15 of the POCSO or 67B of the IT Act.

Upon reviewing the prosecution's records, nothing was gathered during the investigation to indicate that the petitioner purposefully downloaded, viewed, or recorded the video. Additionally, nothing was found to indicate that the petitioner had shared, transmitted, or published the video in any way. The accusation is limited to the accused's cell phone being the only device with pornographic material on it.

- The learnt Single Judge of the Kerala High Court held in **Akhil Johny v. State of Kerala**, reported in 2024 KER 53767, that no offence could be said to have been made out under Section(s) 15 of the POCSO or 67B of the IT Act if the allegations were limited to the presence of pornographic material involving a child on the accused's hard drive or mobile phone. As a result, the criminal proceedings would be subject to being quashed.

Upon reviewing the prosecution's records, nothing was gathered during the investigation to indicate that the petitioner purposefully downloaded, viewed, or recorded the video. Additionally, nothing was found to indicate that the petitioner had shared, transmitted, or published the video in any way. The accusation is limited to the accused's cell phone being the only device with pornographic material on it.

In the Supreme Court of India

Criminal Appellate Jurisdiction

Criminal Appeal no. 2161-2162 Of 2024 (ARISING OUT OF SPECIAL LEAVE PETITION (CRL) NOS. 3665-3666 OF 2024) JUST RIGHTS FOR CHILDREN ALLIANCE V.S. HARISH & ORS, 23 SEPTEMBER 2024

Bench:- CJI, D. Y. Chandrachud Justice, J.B. Pardiwala

In the above-mentioned case the supreme court held that mere viewing, possession and storage of material depicting minors engaged in sexual activity constitutes an offence under the POCSO, 2012. The ruling resolves a protracted dispute between High Courts about the applicability of Section 67B of the Information Technology Act, 2000 (the "IT Act") and Section 15 of the POCSO Act to the "mere storage" of "child pornography." Specifically, it rejected the Madras High Court's ruling in *S Harish v. Inspector of Police and Others* (2024),

which had halted criminal proceedings against a POCSO accused after determining that neither the POCSO nor the IT Act penalised downloading or viewing "child pornography" in and of itself. According to Section 15(1) of the POCSO Act, "anyone, who stores or possesses" "child pornography" and "fails to delete or destroy or report" it may be fined up to 5,000 rupees, and on a further offence, up to 10 thousand rupees. According to Section 15(2), there is a harsher penalty of up to three years in jail if the possession and storage are done with the intention of "transmitting or propagating or displaying or distributing." Numerous High Courts have ruled that in order to prove a Section 15 violation, it was necessary to establish the purpose to disseminate or utilise the content for commercial gain. The Supreme Court made it clear that each of Section 15's subsections defines distinct offences.

Child pornography is illegal to "publish" or "transmit" according to Section 67B of the IT Act. The Court decided that Section 67B penalises the "creation, possession, propagation and consumption of such material" in addition to the "electronic dissemination" of child pornographic content. Judge Pardiwala discussed the necessity to stop using the phrase "child pornography" and replace it with "child sexual exploitative and abuse material," since the latter term better captures the reality of these crimes. He suggested that the POCSO Act be amended by the Parliament to replace the phrases. During the announcement of the Order, the Chief Justice thanked Justice Pardiwala for providing a "landmark judgement."

The petitioner's solicitors agreed right away. Senior Advocate H.S. Phoolka, representing the petitioner, stated, "I think probably in the world, this is the first time this is being dealt with,"

CHAPTER V:

CONCLUSION AND SUGGESTION

5.1. Summary of Key Findings

This research has delved into the duality of technology, especially social media, as both a tool of empowerment and a facilitator of abuse. At the heart of this inquiry lies the paradox of connectivity: while social media provides an unprecedented platform for self-expression, community building, and activism, it simultaneously enables new forms of harassment particularly **cyberbullying and cyberstalking**. The findings across all chapters converge on one undeniable truth: **social media platforms, if left unchecked, can become dangerous spaces where users especially vulnerable populations are exposed to relentless psychological harm**. The examination of **Indian legal frameworks** including the Information Technology Act, 2000, the Indian Penal Code, and the POCSO Act revealed that the current

system is ill-equipped to keep up with the rapid evolution of cybercrimes. Several provisions are outdated, ambiguously worded, or narrowly applied, leading to low rates of prosecution and conviction. Even when laws exist on paper, enforcement mechanisms are either poorly implemented or unavailable to those in need. The technological design of platforms exacerbates the problem. Features such as **anonymous handles, disappearing messages, and encrypted chats** are marketed as privacy enhancements but are often manipulated to harass users without accountability. Women, children, LGBTQ+ individuals, and public figures are disproportionately affected, facing a spectrum of abuse ranging from unsolicited messages to deepfake pornography and death threats.

A comparative analysis with international legislative efforts like the **UK's Online Safety Bill**, the **USA's Stop Cyberstalking Bill (proposed)**, and the **EU's Digital Services Act (DSA)** demonstrates a growing global recognition of platform accountability. These frameworks emphasize **transparency, proactive monitoring, and victim-centric redress mechanisms**, which India's current laws largely lack. Finally, digital forensic tools like **Autopsy, EnCase, FTK, and Cellebrite** offer powerful means to trace perpetrators and preserve evidence. Yet, the **shortage of trained personnel, technical limitations, and jurisdictional issues** significantly hinder effective forensic investigation in India.

5.2. Reflection on the Hypothesis

The core hypothesis of this study posited that **social media, while neutral in its foundational intent, has become a double-edged sword serving both as a vehicle for social good and a conduit for cyber harassment**. This hypothesis has been thoroughly validated. Social media's openness and immediacy offer empowerment, but in the absence of regulatory safeguards, they also become grounds for targeted harassment. Despite existing laws and safety features, the rate of cyberbullying and cyberstalking continues to rise. Survivors often find themselves retraumatized by insensitive policing, lack of technical support, and dismissive platform responses. The hypothesis also suggested that India's current legal and policy responses are **inadequate, reactive, and fragmented** a conclusion that this research strongly affirms. The disjointed relationship between law enforcement, judicial interpretation, platform cooperation, and victim support mechanisms has led to a broken cycle of justice. The absence of real-time redressal mechanisms and effective deterrents emboldens perpetrators and silences victims. Thus, the hypothesis stands confirmed: **Technology, while transformative, is being used as a weapon in the absence of accountability, regulation, and awareness**.

5.3. The Balance Between Free Speech and Online Safety

A recurring theme throughout this research has been the **delicate yet essential balance between free expression and digital safety**. The right to freedom of speech, enshrined in **Article 19(1)(a)** of the Indian Constitution, is fundamental to any democratic society. However, **Article 19(2)** permits reasonable restrictions, especially in the interest of public order, decency, and morality. Cyberbullying and cyberstalking directly infringe upon an individual's **right to life with dignity under Article 21**. These acts are not merely annoying inconveniences they are invasive, repetitive, and emotionally devastating violations of personal space and autonomy. The current regulatory approach, however, fails to strike the necessary balance. Platforms often err on the side of over-permissiveness, allowing harmful content to flourish under the guise of free speech. On the flip side, government mandates sometimes push for blanket censorship, raising fears of authoritarian overreach.

What is needed is **a principled, transparent, and evidence-based content moderation system**. Regulations must ensure platforms develop clear, publicly accessible guidelines that differentiate between **legitimate expression** and **targeted abuse**. Users should also have the right to **appeal content takedown decisions** and receive meaningful explanations for platform actions. This balance is not just legal it is moral. The digital world must become a space where individuals can speak freely without living in fear.

5.4. Policy and Legal Reform Suggestions

Based on the critical insights obtained throughout this research, the following **multi-pronged reform strategy** is proposed:

a) Mandatory Content Moderation Transparency

Platforms should be legally obligated to **publish quarterly transparency reports** that disclose:

- Number of user reports received.
- Time taken to address them.
- Specific categories of action (takedown, warning, account suspension).
- Number of appeals filed and outcomes.

Independent **regulatory audits** should be conducted to assess the consistency and fairness of moderation practices. These reports must be publicly accessible to promote accountability.

b) Robust Cyber Helpline Infrastructure

Victims often struggle with where and how to report abuse. A nationwide **24/7 cyber helpline**, linked to regional cyber cells and legal aid centres, must be established. Key features should include:

- Multilingual support.
- Access to trained counsellors, legal advisors, and technical experts.
- Ability to file police complaints digitally and track progress.

c) Enhanced Training for Law Enforcement in Digital Forensics

Currently, very few law enforcement officers in India are trained to handle digital evidence or understand the nuances of online harassment. There is a dire need for:

- **Mandatory digital forensics training programs** for police academies.
- **On-ground cyber experts** stationed at every police district headquarters.
- **Specialized cyber courts** to expedite digital abuse cases.

This will ensure that complaints are taken seriously, investigated thoroughly, and prosecuted efficiently.

d) Education and Awareness Campaigns

Digital abuse must be addressed not only legally but **culturally and socially**. To do so:

- **Digital citizenship modules** should be introduced in school and college curricula.
- National campaigns (TV, social media, radio) should promote respectful online conduct, the importance of consent, and safe reporting channels.
- Influencers and content creators should be encouraged to act as **ambassadors for digital safety**.

These campaigns can de-stigmatize victimhood, reduce normalisation of online abuse, and cultivate a culture of **compassionate engagement**.

5.5. Final Thoughts: The Path Forward for a Safer Digital Ecosystem

As this research concludes, it becomes evident that the **future of a safer internet lies not in banning platforms or silencing voices, but in designing better systems of accountability, support, and empathy**. The internet is not merely a technological construct it is an **emotional, psychological, and social ecosystem**. With one of the world's largest populations of internet users and a rapidly digitizing society, the urgency to act is **now**. Policymakers must rise above

partisan debates and platform interests to craft laws that are inclusive, forward-looking, and victim-sensitive. Social media companies must also recognize that **profit cannot come at the cost of safety**. It is time they invested seriously in **human moderation, ethical AI, and responsive grievance redressal**. A truly inclusive digital world is one where **freedom of expression thrives not in chaos, but in safety**. A world where children can explore, women can express, and all individuals regardless of gender, sexuality, caste, or identity can exist without fear. Let us not wait for another tragedy to act. Let this be the moment where **law, technology, and humanity converge to reclaim the internet as a force for good**.

BIBLIOGRAPHY

1. Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
2. Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).
3. Protection of Children from Sexual Offences Act, 2012, No. 32, Acts of Parliament, 2012 (India).
4. S. Harish S/o. Santhanam v. The Inspector of Police, 2024 SCC OnLine Mad 11925 (India).
5. Just Rights for Children Alliance v. S. Harish & Ors., 2024 SCC OnLine Mad 11926 (India).
6. United Nations Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.
7. Online Safety Bill, Bill [262] 2023-24, Parliament of the United Kingdom.
8. Stop Cyberstalking Bill, H.R. 6527, 117th Cong. (2022) (U.S.).
9. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act).
10. Rajat Kathuria & Smriti Parsheera, Regulation of Social Media Platforms: A Comparative Study of Germany, Australia, EU, and India, 14 Ind. J.L. & Tech. 82 (2022).
11. Pavan Duggal, Cyber Law: The Indian Perspective (6th ed. 2023).
12. Aparna Viswanathan, Cyber Law: Indian and International Perspectives on Key Topics Including Data Privacy and Cybercrime (LexisNexis 2017).
13. Ashok K. Pandey, Cyber Crime and Law (Central Law Publications 2022).
14. Ministry of Electronics & Information Technology, India, Guidelines for Intermediaries and Digital Media Ethics Code Rules, 2021.

15. Ministry of Women and Child Development, Report on Child Online Protection in India (2022).
16. Anja Kovacs, Internet Governance and Freedom of Expression in India, Internet Democracy Project (2020).
17. A Narrative Review of Cyberbullying Among Indian Adolescents, Nat'l Libr. Med. (2024), <https://pmc.ncbi.nlm.nih.gov/articles/PMC11376467>.
18. Cyberbullying on Social Networks – A Crime in India, Indian J. Psychol. (2024), <https://ijip.in/wp-content/uploads/2024/07/18.01.051.20241203.pdf>.
19. Cyberbullying and Cyberstalking: Their Influence on Teenagers in India, J. Res. Transdisciplinary Disabilities (2024), <https://jrtdd.com/index.php/journal/article/view/3486>.
20. Cyberbullying Legislation in India: Effectiveness and International Comparisons, SSRN (2024), <https://papers.ssrn.com/sol3/Delivery.cfm/5001936.pdf>.
21. Muthamilselvan R., Cyber Forensics: Techniques and Practices in India, 6 Int'l J. Comp. & Cyber Security 29 (2023).
22. Ishita Chatterjee, Impact of End-to-End Encryption on Cyber Crime Investigation, 8 NLUD J. Legal Stud. 112 (2023).
23. Sweta Mohanty, Challenges in Digital Evidence Collection: An Indian Perspective, 14 NUJS L. Rev. 202 (2022).
24. Vaibhav Rana, Cyberstalking and the Indian Legal Response, 2 Indian J. Criminology & Forensic Sci. 45 (2022).
25. The Phenomena of Cyber Bullying and Cyber Stalking, Glob. Media J. (2024), <https://www.globalmediajournal.com/open-access/disturbing-psychosocial-trends-in-social-media-the-phenomena-of-cyber-bullying-and-cyber-stalking.pdf>.
26. R. P. Saini, Investigation of Cybercrime with Forensic Tools: Challenges and Opportunities, 3 Indian Cybersecurity J. 49 (2023).
27. Cyberbullying and Cyberstalking: A Comparative Review Between USA and India, J. Cyber L. & Pol'y (2023).
28. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
29. Supreme Court Guidelines on Preventing Child Sexual Exploitation Material, (2023) 6 SCC 519 (India).
30. Vanya Rakesh, The Safe Harbor Debate: Platform Immunity vs. User Rights in Indian Cyberspace, 7 J. Indian L. & Pol'y 78 (2023).

- ¹ The Internet: A Double-Edged Sword, MORUNGEXPRESS, <https://morungexpress.com/the-internet-a-double-edged-sword> (last visited Apr 26, 2025).
- ² Daisy Mui Hung Kee, Maryam Ammar Lutf Al-Anesi & Sarah Ammar Lutf Al-Anesi, *Cyberbullying on Social Media under the Influence of COVID-19*, 41 GLOBAL BUSINESS AND ORGANIZATIONAL EXCELLENCE 11 (2022), <https://pmc.ncbi.nlm.nih.gov/articles/PMC9350190/> (last visited Apr 26, 2025).
- ³ “A Review of the Research on Children and Young People Who Display Harmful Sexual Behaviour Online (HSB) | NSPCC Learning” (NSPCC Learning) <<https://learning.nspcc.org.uk/research-resources/2016/review-children-young-people-harmful-sexual-behaviour-online?form=MG0AV3>>
- ⁴ Aastha Johri & Dr Rajiv Singh, *Cyberbullying on Social Networks – A Crime in India*.
- ⁵ Rachna & Dr Rahul Varshney, *Cyberbullying And Cyberstalking: Their Influence on The Social and Emotional Development of Teenagers in India*, 6 JRTDD 1357 (2023), <https://jrtdd.com/index.php/journal/article/view/3486> (last visited Apr 26, 2025).
- ⁶ Rachna & Dr Rahul Varshney, *Cyberbullying And Cyberstalking: Their Influence on The Social and Emotional Development of Teenagers in India*, 6 JRTDD 1357 (2023), <https://jrtdd.com/index.php/journal/article/view/3486> (last visited Apr 26, 2025).
- ⁷ Prithwish Ganguli, *Cyberbullying Legislation in India: Effectiveness and International Perspectives* (2024), <https://papers.ssrn.com/abstract=5001936> (last visited Apr 26, 2025).
- ⁸ (PDF) A systematic literature review on cyberstalking. An analysis of past achievements and future promises, RESEARCHGATE (2024), https://www.researchgate.net/publication/347381968_A_systematic_literature_review_on_cyberstalking_An_an_alysis_of_past_achievements_and_future_promises (last visited Apr 26, 2025).
- ⁹ View of CYBERBULLYING AND CYBERSTALKING: BELONGINGS AND ANTICIPATION MEASURES IN INDIA, https://www.granthaalayahpublication.org/Arts-Journal/ShodhKosh/article/view/4289/3860?utm_source=chatgpt.com (last visited Apr 26, 2025).
- ¹⁰ Cyberbullying Amongst Teenagers in India: Addressing the Issue with the Information Technology Act of 2000
- ¹¹ LWL | Cyberbullying amongst teenagers in India: Addressing the Issue w, HSA TUTORING (2024), <https://tutoring.hsa.net/blogs/students-published-works/lwl-cyberbullying-amongst-teenagers-in-india-addressing-the-issue-with-the-information-technology-act-of-2000> (last visited Apr 26, 2025).
- ¹² Adithya Manikandan, *The Legal Landscape of Cyberbullying and Social Media Privacy: Challenges and Opportunities to Protect Children*, 12 (2025).
- ¹³ Ganguli, *supra* note 7.
- ¹⁴ Helpline Numbers - CSR India, (May 14, 2021), <https://www.csrindia.org/helpline-numbers/> (last visited Apr 26, 2025).
- ¹⁵ Technology-Facilitated Domestic and Sexual Violence: A Review - Nicola Henry, Asher Flynn, Anastasia Powell, 2020, <https://journals.sagepub.com/doi/10.1177/1077801219875821> (last visited Apr 26, 2025).
- ¹⁶ Are we braver in cyberspace? Social media anonymity enhances moral courage, 148 COMPUTERS IN HUMAN BEHAVIOR 107880 (2023), <https://www.sciencedirect.com/science/article/abs/pii/S0747563223002315> (last visited Apr 26, 2025).
- ¹⁷ Exploring the impact of cyberbullying and cyberstalking on victims' behavioural changes in higher education during COVID-19: A case study, 75 INTERNATIONAL JOURNAL OF LAW, CRIME AND JUSTICE 100628 (2023), <https://www.sciencedirect.com/science/article/pii/S175606162300054X> (last visited Apr 26, 2025).
- ¹⁸ *Id.*
- ¹⁹ Manikandan, *supra* note 12.
- ²⁰ Charisse L. Nixon, *Current Perspectives: The Impact of Cyberbullying on Adolescent Health*, 5 ADOLESCENT HEALTH, MEDICINE AND THERAPEUTICS 143 (2014), <https://pmc.ncbi.nlm.nih.gov/articles/PMC4126576/> (last visited Apr 28, 2025).
- ²¹ Social Drivers and Algorithmic Mechanisms on Digital Media - Hannah Metzler, David Garcia, 2024, <https://journals.sagepub.com/doi/10.1177/17456916231185057> (last visited Apr 28, 2025).
- ²² Cyberstalking - Cyberbullying Research Center, <https://cyberbullying.org/cyberstalking> (last visited Apr 28, 2025).
- ²³ Srivastav, T. (2024) *Online ghost: How threat actors secure and hide their IP addresses with proxy, VPN, and tor, The420.in*. Available at: <https://the420.in/online-ghost-how-threat-actors-secure-and-hide-their-ip-addresses-with-proxy-vpn-and-tor/> (Accessed: 26 April 2025).
- ²⁴ Mandatory Verification of Social Media Accounts, <https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1882060> (last visited Apr 26, 2025).
- ²⁵ Matthew N. Berger et al., *Social Media Use and Health and Well-Being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review*, 24 JOURNAL OF MEDICAL INTERNET RESEARCH e38449 (2022),

<https://pmc.ncbi.nlm.nih.gov/articles/PMC9536523/> (last visited Apr 26, 2025).

²⁶ Women Journalists Face Massive Online Abuse: IFJ Report, <https://iju.org.in/campaigns/gender-equality/90-women-journalists-face-massive-online-abuse-ifj-report> (last visited Apr 28, 2025).

²⁷ Sexual identity, gender, and anticipated discrimination in prosocial behavior, 154 EUROPEAN ECONOMIC REVIEW 104427 (2023), <https://www.sciencedirect.com/science/article/pii/S0014292123000569> (last visited Apr 28, 2025).

²⁸ Lasse Brandt et al., *The Effects of Social Isolation Stress and Discrimination on Mental Health*, 12 TRANSLATIONAL PSYCHIATRY 398 (2022), <https://pmc.ncbi.nlm.nih.gov/articles/PMC9490697/> (last visited Apr 28, 2025).

²⁹ Anxiety Disorders - National Institute of Mental Health (NIMH), <https://www.nimh.nih.gov/health/topics/anxiety-disorders> (last visited Apr 28, 2025).

³⁰ kbadqkdclswfjdelrquehwuxcfmijmuixngudufgububgubfugbububjxcgfvbsdihbgfGhdfgFHtyhRtMjk4NzY=.pdf, <https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdclswfjdelrquehwuxcfmijmuixngudufgububgubfugbububjxcgfvbsdihbgfGhdfgFHtyhRtMjk4NzY=> (last visited Apr 28, 2025).

³¹ Parvejur Rahman & Sagufta Mehnaz, *International Journal for Multidisciplinary Research (IJFMR)*, SSRN JOURNAL (2024), <https://www.ssrn.com/abstract=5054029> (last visited Apr 28, 2025).

³² Behind the screens: Understanding the gaps in India's fight against online child sexual abuse and exploitation, 4 CHILD PROTECTION AND PRACTICE 100088 (2025), <https://www.sciencedirect.com/science/article/pii/S2950193824000883> (last visited Apr 28, 2025).

³³ Indian judicial precedents play a significant role in shaping the interpretation and application of laws related to cyberbullying and cyberstalking. Courts have increasingly acknowledged the need for a more robust legal framework to address online harassment and digital abuse, particularly through landmark judgments. - Google Search,

https://www.google.com/search?q=Indian+judicial+precedents+play+a+significant+role+in+shaping+the+interpretation+and+application+of+laws+related+to+cyberbullying+and+cyberstalking.+Courts+have+increasingly+acknowledged+the+need+for+a+more+robust+legal+framework+to+address+online+harassment+and+digital+abuse%2C+particularly+through+landmark+judgments.&oq=Indian+judicial+precedents+play+a+significant+role+in+shaping+the+interpretation+and+application+of+laws+related+to+cyberbullying+and+cyberstalking.+Courts+have+increasingly+acknowledged+the+need+for+a+more+robust+legal+framework+to+address+online+harassment+and+digital+abuse%2C+particularly+through+landmark+judgments.&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzgwMmowajeoAgCwAgA&sourceid=chrome&ie=UTF-8 (last visited Apr 28, 2025).

³⁴ K.S. Puttaswamy v. Union of India (2017)

³⁵ Shreya Singhal v. Union of India (2015)

³⁶ State v. S. Harish (2024)

³⁷ What is digital forensics? | IBM, <https://www.ibm.com/think/topics/digital-forensics> (last visited Apr 28, 2025).

³⁸ Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review, <https://www.mdpi.com/2073-431X/13/8/213> (last visited Apr 28, 2025).

³⁹ Role of Digital Forensic in solving cyber crimes, RESEARCHGATE, https://www.researchgate.net/publication/360919194_Role_of_Digital_Forensic_in_solving_cyber_crimes (last visited Apr 28, 2025).

⁴⁰ Social Media Impact: How Social Media Sites Affect Society, <https://www.apu.apus.edu/area-of-study/business-and-management/resources/how-social-media-sites-affect-society/> (last visited Apr 28, 2025).

⁴¹ How transparent are transparency reports? Comparative analysis of transparency reporting across online platforms, 47 TELECOMMUNICATIONS POLICY 102477 (2023),

<https://www.sciencedirect.com/science/article/pii/S0308596122001793> (last visited Apr 28, 2025). ⁴² Algorithmic content moderation: Technical and political challenges in the automation of platform governance

- Robert Gorwa, Reuben Binns, Christian Katzenbach, 2020, <https://journals.sagepub.com/doi/10.1177/2053951719897945> (last visited Apr 28, 2025).

⁴³ Sexual Harassment & Self-Destructing Messages: Challenges & Evidence, <https://poshatwork.com/sexual-harassment-self-destructing-messages-challenges-evidence/> (last visited Apr 28, 2025).

⁴⁴ 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), <https://link.springer.com/article/10.1007/s10639-022-11168-4> (last visited Apr 28, 2025).

⁴⁵ H.R.6035 - 118th Congress (2023-2024): Stop Electronic Stalking Act | Congress.gov | Library of Congress, <https://www.congress.gov/bill/118th-congress/house-bill/6035> (last visited Apr 28, 2025).

⁴⁶ Your DSA Legal Representative in the EU | Prighter, https://prighter.com/product/dsa/?utm_source=google&utm_medium=cpc&utm_campaign=DSA-Rep-G-S-precision&utm_term=compliance&gad_source=1&gbraid=0AAAAAC_IJIW_NfhjWwtRgwDntbjnfZS4&gclid=EAIaIQobChMIInNLtx6j6jAMVtMw8Ah0pLhLBEAAYASAAEgL0nfD_BwE (last visited Apr 28, 2025).

⁴⁷ Best Practices | NFS, <https://www.nitforstates.gov.in/best-practice-landing> (last visited Apr 28, 2025).

⁴⁸ Supreme Court Observer, “Supreme Court Holds That Viewing, Storing and Possessing ‘Child Pornography’ Is Punishable under POCSO Act; Overturns Madras HC Decision - Supreme Court Observer” (*Supreme Court Observer*, September 24, 2024) <<https://www.scobserver.in/journal/supreme-court-holds-that-viewing-storing-and-possessing-child-pornography-is-punishable-under-pocso-act-overturns-madras-hc-decision/>>.

⁴⁹ Victimization Consequences, Levels of Impact & Examples - Lesson | Study.com, <https://study.com/academy/lesson/victimization-consequences-emotional-psychological-social.html> (last visited Apr 28, 2025).

⁵⁰ Understanding the role of digital technologies in education: A review, 3 SUSTAINABLE OPERATIONS AND COMPUTERS 275 (2022), <https://www.sciencedirect.com/science/article/pii/S2666412722000137> (last visited Apr 28, 2025).

⁵¹ CRL.O. P No.37 of 2024

⁵² CRL.O.P No.37 of 2024

