



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.

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.

STUDY ON CYBER HARASSMENT AGAINST WOMEN IN INDIA

AUTHORED BY - ABIMANYU M

TABLE OF CASES

S. No.	Name of the Case	Year
1	<i>State of Tamil Nadu v. Suhas Katti</i>	2004
2	<i>Avnish Bajaj v. State (NCT of Delhi)</i>	2012
3	<i>Shreya Singhal v. Union of India</i>	2015
4	<i>Sharat Babu Digumarti v. Government of NCT of Delhi</i>	2017
5	<i>Justice K.S. Puttaswamy (Retd.) v. Union of India</i>	2017
6	<i>Sabu Mathew George v. Union of India</i>	2017
7	<i>Nipun Saxena v. Union of</i>	2018

WHITE BLACK
LEGAL

CHAPTER I – INTRODUCTION

1.1 Background of the Study

The internet and social media have become an important part of everyday life. Women use digital platforms for communication, education, employment, business and entertainment. However, the increasing use of digital technology has also created opportunities for online abuse and harassment. Cyber harassment against women may take different forms, such as cyber stalking, online threats, impersonation, fake accounts, abusive messages and non-consensual sharing of private content. Cyber harassment can seriously affect a woman's privacy, dignity, reputation and personal safety. It may also restrict her freedom to use social media and other online platforms. In many cases, women may hesitate to report cyber harassment because of fear, social pressure, lack of awareness or fear of further harassment. India has several legal provisions that can be used to deal with cyber-related offences. The Information Technology Act, 2000 provides an important legal framework for offences involving electronic communication and technology. The Bharatiya Nyaya Sanhita, 2023 contains provisions that may apply to offences such as stalking, criminal intimidation and other acts affecting women. The Bharatiya Sakshya Adhiniyam, 2023 is also relevant because electronic records and digital evidence are important in cyber crime cases.¹

However, technology is developing rapidly and new forms of online harassment continue to emerge. This creates challenges in identifying offenders, collecting electronic evidence, determining jurisdiction and ensuring timely investigation. The role and responsibility of digital platforms in preventing and responding to cyber harassment also requires examination². Therefore, this study focuses on cyber harassment against women in India and examines whether the existing legal framework is sufficient to deal with the changing forms of online harassment.

1.2 Significance of the Study

Cyber harassment against women is an important legal and social issue. Online harassment can affect the privacy, dignity, reputation and safety of women. Unlike some forms of physical harassment, harmful online content can be copied, shared and circulated repeatedly, making its impact difficult to control. The study is significant because cyber harassment is changing with

¹ Information Technology Act, 2000, sec 21

² Debarati Halder & K. Jaishankar, *Cyber Crimes Against Women in India* (SAGE Publications 2016).

the development of social media and digital technology. Although legal provisions are available, women may still face practical difficulties in obtaining justice.

Problems such as anonymity of offenders, lack of electronic evidence, jurisdictional issues, delay in investigation and difficulties in removing harmful content can affect the effectiveness of legal remedies. The study is also important from a constitutional perspective.

Cyber harassment may affect women's rights to equality, privacy, dignity and freedom of expression. Therefore, the issue needs to be examined not only under cyber laws but also in relation to constitutional rights. This study will help to understand the strengths and limitations of the existing legal framework and identify areas where legal and institutional measures can be improved.

1.3 Review of Literature

1. **Debarati Halder and K. Jaishankar: Cyber Crimes Against Women in India**, discuss different forms of cyber crimes against women and the legal and social problems associated with them. Their work provides an important understanding of online harassment and the difficulties faced by women in cyberspace.
2. **Pavan Duggal, in Cyber Law: The Indian Perspective**, discusses the Indian cyber-law framework and different cyber offences. His work helps in understanding the legal framework relating to cyber crimes and the challenges created by the changing nature of technology³
3. **Avneet Kaur: Cybercrime Against Women in India: Challenges and Possible Solutions**, discusses cybercrime affecting women and the challenges involved in protecting women in the digital environment. The work also considers possible measures for addressing these challenges.

1.4 Research Gap

Existing studies have discussed cyber crime, online violence, social media abuse, privacy and legal protection available to women in India. However, there is still a need to examine whether the existing Indian legal framework is sufficient to deal with the changing forms of cyber harassment against women. Most of the existing literature deals with individual forms of cyber offences separately. Comparatively less attention has been given to examining cyber stalking, impersonation, online threats, fake accounts, non-consensual sharing of private

³ Pavan Duggal, *Cyber Law: The Indian Perspective* (Saakshar Law Publications 2002).

content and other forms of harassment together. There is also a need to examine the effectiveness of the Information Technology Act, 2000 along with the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. Practical issues such as electronic evidence, anonymity of offenders, jurisdiction, delay in investigation and the responsibility of digital platforms also require further study. The effect of cyber harassment on women's privacy, dignity, equality and freedom of expression also requires greater examination from a constitutional point of view. Therefore, this study seeks to address these gaps through a doctrinal study of the existing legal framework, judicial decisions, constitutional principles, international approaches and practical legal challenges relating to cyber harassment against women in India.

1.5 Research Objectives

The study has the following objectives:

1. To understand the different forms of cyber harassment against women in India.
2. To examine the effectiveness of the existing Indian legal framework relating to cyber harassment against women.
3. To identify the practical challenges relating to electronic evidence, anonymity, jurisdiction, delay in investigation and digital platforms⁴
4. To analyse the impact of cyber harassment on women's constitutional rights and suggest suitable legal and institutional measures for better protection⁵

1.6 Research Questions

The study seeks to answer the following questions:

1. What are the major forms of cyber harassment faced by women in India?
2. Whether the existing Indian legal framework is sufficient to deal with the changing forms of cyber harassment against women?
3. What are the major practical challenges relating to electronic evidence, anonymity, jurisdiction, delay in investigation and digital platforms?
4. How does cyber harassment affect women's constitutional rights, and what measures can improve their legal protection?

⁴ Bharatiya Sakshya Adhiniyam, sec 47 of 2023

⁵ INDIA CONSTITUTION. article 14, 19, 21.

1.7 Research Methodology

This study adopts a doctrinal research methodology. The study is based on the examination and analysis of existing legal materials and does not involve field surveys, questionnaires or personal interviews. The research mainly uses primary and secondary sources to understand the legal position relating to cyber harassment against women in India.

1.7.1 Primary Sources

The primary sources include:

- Constitution of India
- Information Technology Act, 2000
- Bharatiya Nyaya Sanhita, 2023
- Bharatiya Sakshya Adhiniyam, 2023
- Protection of Women from Domestic Violence Act, 2005, wherever relevant
- Judicial decisions of the Supreme Court and High Courts
- Relevant rules, regulations and government materials

1.7.2 Secondary Sources

The secondary sources include:

- Books on cyber law and criminal law
- Research articles
- Law journals
- Reports
- Legal commentaries
- Reliable online legal resources

The collected materials are analysed to understand the existing legal framework, judicial approach and practical challenges relating to cyber harassment against women. Constitutional principles and selected international approaches are also examined for comparison.

The study critically evaluates the existing legal provisions and judicial decisions to identify the strengths, limitations and gaps in the protection available to women against cyber harassment⁶

1.8 Limitations of the Study

1. The study is purely doctrinal and does not include field surveys or personal interviews.
2. The study mainly focuses on the Indian legal framework.
3. International approaches are considered only for comparative purposes.

⁶ Bharatiya Nyaya Sanhita, No. 45 of 2023,

4. Cyber technology changes rapidly, and new forms of cyber harassment may develop over time.
5. The study depends mainly on available legal materials, judicial decisions, books, articles and reports.
6. The study focuses specifically on cyber harassment against women and does not cover every form of cyber crime in detail.

1.9 Scheme of the Study

Chapter I – Introduction explains the background and significance of the study and presents the review of literature, research gap, objectives, research questions, methodology and limitations.

Chapter II – Concept and Forms of Cyber Harassment Against Women explains the meaning, nature and different forms of cyber harassment, including cyber stalking, online threats, impersonation, fake accounts and non-consensual sharing of private content.

Chapter III – Legal Framework and Judicial Approach examines the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Bharatiya Sakshya Adhiniyam, 2023, relevant judicial decisions and the role of digital platforms.

Chapter IV – Constitutional Rights and Challenges examines the impact of cyber harassment on women's equality, privacy, dignity and freedom of expression. It also discusses practical challenges such as anonymity, electronic evidence, jurisdiction, underreporting and delay in investigation.

Chapter V – Critical Analysis, Findings and Suggestions critically evaluates the effectiveness of the existing legal framework, identifies legal and practical gaps, considers selected international approaches and provides findings, suggestions and recommendations for better protection of women against cyber harassment.

CHAPTER II – CONCEPT AND FORMS OF CYBER HARASSMENT AGAINST WOMEN

The growth of the internet and social media has created new forms of harassment against women in the digital environment. Cyber harassment may include stalking, bullying, threats, impersonation, identity theft and sharing of private content without consent. This chapter

explains the meaning, evolution and major forms of cyber harassment against women in India and examines their impact on privacy, dignity and safety. It provides the basic foundation for understanding the legal and practical issues discussed in the following chapters.

2.1 Meaning and Nature of Cyber Harassment

This section explains the meaning, concept and basic nature of cyber harassment against women in the digital environment. It examines how the internet, social media platforms, messaging applications, email services and other digital technologies can be misused to harass, threaten, abuse, monitor, insult or humiliate women. Cyber harassment may involve repeated unwanted communication or a single serious act depending on the nature and effect of the conduct. The section also discusses the important characteristics of cyber harassment, such as its speed, wide reach, persistence and the possibility of anonymous communication. Unlike traditional forms of harassment, online content can be copied, forwarded and shared with a large number of people within a short period. Therefore, cyber harassment can continue to affect a woman even after the original content has been removed. The discussion will help in understanding why cyber harassment has become an important legal and social issue in India.

2.2 Evolution of Cyber Harassment in India

This section traces the development of cyber harassment in India along with the growth of internet access, smartphones, social media and digital communication. In the earlier stages of internet use, online harassment was mainly associated with unwanted emails, abusive messages and other forms of direct communication. With the expansion of social networking platforms and digital services, the methods used for harassment have also become more varied and complex. The section examines the development of fake profiles, impersonation, online threats, cyber stalking, identity misuse and circulation of private content. It also considers how technological developments have created new ways of targeting women online. The changing nature of cyber harassment is important for this study because it raises the question of whether existing Indian laws are sufficient to deal with new and emerging forms of online abuse⁷

2.3 Major Forms of Cyber Harassment Against Women

This section identifies and explains the major forms of cyber harassment experienced by women in India. It includes cyber stalking, online bullying, online threats, intimidation,

⁷ Avneet Kaur, Cybercrime Against Women in India: Challenges and Possible Solutions, in *The Techno-Legal Dynamics of Cyber Crimes in Industry 5.0* (Wiley 2025)

impersonation, identity theft, fake accounts, abusive or defamatory content and non-consensual sharing of private images. Each form may have different characteristics, but they can also be connected and may occur together in the same incident. The purpose of this section is not merely to list different cyber offences but to understand how these forms operate and affect women in practice. Existing discussions often focus on particular forms of cyber offences separately. Therefore, examining the different forms together helps the present study address its research gap and provides a broader understanding of cyber harassment against women⁸

2.4 Cyber Stalking and Online Bullying

This section examines cyber stalking and online bullying as significant forms of harassment faced by women. Cyber stalking may involve repeatedly contacting a woman through online platforms, monitoring her online activities, following her digital presence, sending unwanted messages or making repeated attempts to communicate with her. Such conduct may create fear, discomfort and a feeling of being constantly watched. Online bullying includes abusive comments, insulting messages, humiliating posts, threatening communications and coordinated online attacks. Women may also face repeated trolling and personal attacks on social media. These activities can affect their privacy, dignity, reputation and willingness to participate freely in online spaces. The section therefore examines not only the nature of these forms but also their impact on women.

2.5 Cyber Threats, Impersonation and Identity Theft

This section discusses the use of digital platforms to threaten, intimidate or create fear among women. Online threats may involve threatening messages, abusive communications, threats to disclose private information or other conduct intended to control or frighten the victim. Such threats may sometimes be combined with other forms of cyber harassment. The section also examines impersonation, fake accounts and identity theft. A person may create a false online identity or misuse another person's name, photographs or personal information for various harmful purposes. Impersonation can damage a woman's reputation, deceive her contacts or expose her to further harassment. Identity-related offences also create difficulties in identifying the actual offender, particularly where anonymous accounts or false identities are used. This issue will be connected with the practical challenges of anonymity and investigation discussed in later chapters.

⁸ Information Technology Act, No. 21 of 2000, §§ 66C–67A, India Code (2000).

2.6 Non-Consensual Sharing of Private Images

This section examines the sharing, uploading, forwarding or circulation of private or intimate images without the consent of the woman concerned. Such content may initially be shared with a person in confidence but may later be distributed through social media, messaging applications, websites or other digital platforms without permission. The section explains how non-consensual sharing can seriously affect a woman's privacy, dignity, reputation and personal security. Once digital content is circulated, it may be difficult to identify every person who has copied or shared it and difficult to completely remove it from the internet. The issue therefore raises important questions regarding consent, privacy, removal of unlawful content, responsibility of digital platforms and the availability of effective legal remedies.

2.7 Gender-Based Violence in Cyberspace

This section examines cyber harassment from the broader perspective of gender-based violence. Women may be targeted online through sexual harassment, threats, humiliation, character attacks, abusive comments and other forms of digital abuse because of their gender. Such conduct can discourage women from expressing their opinions, using social media or participating equally in digital spaces. The section also examines the connection between cyber harassment and women's constitutional interests, particularly equality, privacy, dignity and freedom of expression. Cyber harassment is therefore not only an individual online problem but also an issue affecting women's equal and meaningful participation in society.

This discussion provides the foundation for the constitutional analysis and practical challenges that will be examined in the later chapters⁹

This chapter examined the meaning, evolution and major forms of cyber harassment against women in India. It discussed cyber stalking, online bullying, threats, impersonation, identity theft and non-consensual sharing of private images. These forms can seriously affect women's privacy, dignity, safety and freedom of expression. The discussion provides the foundation for the next chapter, which examines the existing legal framework and judicial approach to cyber harassment against women.

⁹ INDIA CONSTITUTION arts. 14, 19(1)(a), 21.

CHAPTER III – LEGAL FRAMEWORK AND JUDICIAL APPROACH

Cyber harassment against women requires an effective legal framework that can respond to the different forms of abuse taking place through digital platforms. In India, protection is provided through the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023, along with relevant rules and judicial decisions. This chapter examines these legal provisions, electronic evidence, cyber crime reporting mechanisms and the responsibility of digital platforms. It also analyses important judicial decisions relating to cyber offences, privacy and online freedom to understand how Indian courts have responded to the changing nature of cyber harassment.

3.1 Information Technology Act, 2000

This section examines the Information Technology Act, 2000 as the main legislation dealing with cyber activities and offences in India. It discusses the provisions relevant to cyber harassment, including the misuse of computer resources, identity-related offences, privacy violations and publication or transmission of unlawful content. The section also considers the extent to which the Act can be applied to different forms of harassment faced by women through social media and other digital platforms. The changing nature of cyber offences has created situations that may not always fit easily within older legal provisions. Therefore, this section also examines the strengths and limitations of the Information Technology Act in providing effective protection to women against emerging forms of cyber harassment.

3.2 Relevant Provisions of Bharatiya Nyaya Sanhita, 2023

This section examines the relevant provisions of the Bharatiya Nyaya Sanhita, 2023 that may apply to cyber harassment against women. It considers offences involving stalking, criminal intimidation, sexual harassment, defamation, insulting or threatening conduct and other forms of abuse that may be committed through digital platforms. The section explains how the BNS operates along with the Information Technology Act when an act of harassment has both cyber and general criminal law aspects. It also considers whether the existing criminal law provisions are adequate to respond to new forms of online harassment and whether there are practical difficulties in applying traditional offences to digital conduct.

3.3 Bharatiya Sakshya Adhiniyam, 2023 and Electronic Evidence

Electronic evidence is particularly important in cyber harassment cases because the offence may take place entirely through digital platforms. This section examines the provisions of the Bharatiya Sakshya Adhiniyam, 2023 relating to electronic and digital records. It discusses the evidentiary value of screenshots, emails, messages, social media posts, photographs, videos, account details and other digital records. The section also considers practical difficulties relating to the collection, preservation, authentication and production of electronic evidence before courts. Issues such as deletion of online content, alteration of digital records and difficulty in obtaining information from platforms may affect the successful investigation and prosecution of cyber harassment cases.

3.4 Cyber Crime Reporting Mechanisms

This section examines the mechanisms available in India for reporting cyber harassment and other cyber crimes. It discusses the role of cyber crime police stations, online reporting facilities and other authorities involved in receiving and investigating complaints. The availability of simple and accessible reporting mechanisms is particularly important for women who may hesitate to approach the police because of fear, social pressure or lack of legal awareness. The section also considers practical problems such as delay in registration or investigation, lack of awareness about reporting procedures and difficulties in approaching the appropriate authority. These issues are relevant to the research gap because the existence of legal provisions alone may not ensure effective protection unless women are able to access and use the available remedies¹⁰

3.5 Intermediary Responsibility and Digital Platforms

This section examines the responsibility of social media platforms, messaging applications, websites and other digital intermediaries in dealing with cyber harassment. Digital platforms may play an important role in receiving complaints, restricting harmful accounts, removing unlawful content and preserving relevant information for investigation. The section also considers the challenges involved in holding platforms responsible for harmful online content while maintaining freedom of expression and legitimate online communication. The effectiveness of reporting and content-removal mechanisms, cooperation with law enforcement authorities and protection of users from repeated harassment are examined as

¹⁰ Ministry of Home Affairs, Government of India, New Criminal Laws, <https://www.mha.gov.in/en/commoncontent/new-criminal-laws> (last visited Sept. 14, 2026).

important aspects of platform responsibility¹¹

3.6 Important Judicial Decisions

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

State of Tamil Nadu v. Suhas Katti is one of the early important Indian cases involving cyber harassment of a woman. The accused posted obscene and defamatory messages about the victim on a Yahoo message group and used her name to cause humiliation. The court convicted the accused under the Information Technology Act, 2000 and the Indian Penal Code. The case is significant because it shows how electronic communication can be used to harass and defame women. It also demonstrates the importance of electronic evidence in establishing cyber offences¹²

3.6.2 Avnish Bajaj v. State (NCT of Delhi) (2012)

This case concerned the liability of the person associated with the operation of the Baazee.com website after an obscene video was listed for sale through the platform. The case raised important questions regarding the responsibility of intermediaries for unlawful content uploaded by users. It is relevant to the present study because digital platforms can be misused for the circulation of abusive or unlawful content against women. The case highlights the need to examine the responsibility of online platforms while dealing with cyber offences¹³

3.6.3 Shreya Singhal v. Union of India (2015)

In this landmark decision, the Supreme Court struck down Section 66A of the Information Technology Act, 2000 as unconstitutional. The Court held that the provision violated the freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution. The judgment is important in cyber law because it established that restrictions on online speech must satisfy constitutional requirements. In cases of cyber harassment, the judgment requires a balance between protecting individuals from unlawful online abuse and protecting legitimate freedom of expression.

3.6.4 Sharat Babu Digumarti v. Government of NCT of Delhi (2017)

This case dealt with the relationship between the Information Technology Act and the Indian Penal Code in relation to offences involving electronic content. The Supreme Court considered the special nature of the Information Technology Act and held that where an offence is

¹¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

¹² *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004 (Addl. Chief Metro. Magistrate, Egmore, Chennai Nov. 5, 2004).

¹³ *Avnish Bajaj v. State (NCT of Delhi)*, 2004 SCC OnLine Del 1160 : (2005) 79 DRJ 576, rev'd on other grounds, Criminal Appeal No. 1483 of 2009 (S.C. Apr. 27, 2012).

specifically covered by the IT Act, the special law would prevail over the general provisions of the IPC in the circumstances considered by the Court. The decision is relevant to cyber harassment because it shows the importance of applying the specialised cyber law framework when dealing with offences committed through electronic means.

3.6.5 Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

In this landmark constitutional judgment, the Supreme Court recognised the right to privacy as a fundamental right under Article 21 and other constitutional guarantees. Privacy includes protection of personal autonomy, dignity and control over personal information. The judgment is highly relevant to cyber harassment against women because online stalking, unauthorised use of personal information and sharing of private content can seriously affect a person's privacy and dignity¹⁴

3.6.6 Sabu Mathew George v. Union of India (2017)

This case concerned the availability and display of pre-natal sex determination advertisements through online search engines. The Supreme Court directed search engines to take effective steps to prevent prohibited advertisements from appearing on their platforms. The decision is relevant to the present study because it demonstrates that digital platforms may have responsibilities in preventing unlawful content from being made easily accessible online. It also highlights the importance of cooperation between courts, authorities and online platforms.

3.6.7 Nipun Saxena v. Union of India (2018)

In *Nipun Saxena v. Union of India*, the Supreme Court issued important directions concerning the protection of the identity and privacy of victims of sexual offences. The Court emphasised that the identity of victims should not be disclosed in a manner that could lead to their identification. The case is relevant to cyber harassment because personal information and sensitive details can easily be circulated through digital platforms. Protection of victim identity is therefore an important aspect of privacy, dignity and effective legal protection¹⁵

3.7 Judicial Approach towards Privacy and Online Freedom

The Indian judiciary has played an important role in balancing privacy, dignity, freedom of expression and protection from online abuse. Courts have recognised that the digital environment provides individuals with an important platform to communicate, express opinions and participate in public discussions. At the same time, online freedom cannot be used as a justification for unlawful harassment, threats, privacy violations or circulation of

¹⁴ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

¹⁵ Nipun Saxena v. Union of India, (2019) 2 SCC 703.

prohibited content. The decision in *Shreya Singhal v. Union of India* is particularly important for understanding the protection of online freedom. The Supreme Court recognised the constitutional importance of freedom of speech and expression on the internet and struck down Section 66A of the Information Technology Act, 2000. This shows that restrictions on online communication must comply with constitutional standards. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy as a fundamental right. This principle has significant relevance to cyber harassment against women because activities such as cyber stalking, misuse of personal information, unauthorised sharing of private images and online monitoring can interfere with privacy and dignity. The courts have also recognised the importance of controlling unlawful online content and protecting victims. Decisions such as *Sabu Mathew George* and *Nipun Saxena* demonstrate the need for appropriate responsibilities on digital platforms and protection of sensitive information. Therefore, the judicial approach attempts to maintain a balance between online freedom and individual protection. Overall, judicial decisions show that constitutional rights continue to apply in the digital environment. However, judicial protection alone may not be sufficient to address the rapidly changing forms of cyber harassment. Effective implementation of laws, proper handling of electronic evidence, identification of anonymous offenders and cooperation from digital platforms are also necessary for providing effective protection to women.

This chapter examined the Indian legal framework and judicial approach relating to cyber harassment against women. The discussion shows that existing laws provide remedies for several forms of online harassment, while electronic evidence, reporting mechanisms and digital platform responsibility remain important for effective enforcement. Judicial decisions have also played an important role in protecting privacy, dignity and online freedom.

However, the changing nature of cyber harassment creates practical difficulties that require further attention, which are examined in the following chapter¹⁶

CHAPTER IV – CONSTITUTIONAL RIGHTS AND CHALLENGES

Cyber harassment against women is not only a legal issue but also a matter of constitutional rights and practical difficulties. Online threats, stalking, abuse and privacy violations can affect women's equality, freedom of expression, privacy and dignity. This chapter examines these

¹⁶ Sharat Babu Digumarti v. Govt. of NCT of Delhi, (2017) 2 SCC 18; Sabu Mathew George v. Union of India, (2017) 7 SCC 657.

constitutional concerns along with practical challenges such as lack of awareness, underreporting, anonymity, electronic evidence, jurisdiction and delays in investigation. It also considers how these challenges affect the effective protection of women against cyber harassment.

4.1 Cyber Harassment and Article 14

This section examines the relationship between cyber harassment and the constitutional guarantee of equality under Article 14 of the Constitution of India. Women who face online harassment may experience unequal treatment, discrimination and restrictions on their participation in digital spaces. The section considers whether cyber harassment can affect women's ability to use digital platforms equally and safely. It also examines the importance of equal legal protection for women facing cyber harassment. The discussion helps to understand whether existing legal and institutional responses provide adequate protection to women without discrimination and whether stronger measures are required to ensure equality in the digital environment¹⁷

4.2 Cyber Harassment and Article 19

This section examines the impact of cyber harassment on the freedom of speech and expression guaranteed under Article 19(1)(a). The internet and social media have become important platforms through which women express their views, share information and participate in public discussions. However, continuous trolling, threats, abusive comments and online attacks may discourage women from expressing themselves freely. The section also considers the need to balance freedom of expression with reasonable restrictions and protection from unlawful online abuse. The objective is to understand how the fear of harassment can create a situation where women choose to remain silent or withdraw from online platforms¹⁸

4.3 Cyber Harassment and Article 21

This section examines cyber harassment in relation to the right to life and personal liberty under Article 21. The right to life has been interpreted broadly by the courts to include important aspects of human dignity and personal security. Online threats, stalking, humiliation and misuse of private information can seriously affect a woman's sense of safety and dignity. The section therefore considers how cyber harassment may interfere with a woman's ability to live

¹⁷ INDIA CONSTITUTION. art. 14.

¹⁸ Shreya Singhal v. Union of India, (2015) 5 SCC 1.

with dignity and personal security. It also examines the importance of effective legal remedies and institutional protection in safeguarding these interests in the digital environment.

4.4 Right to Privacy and Dignity

This section focuses specifically on the right to privacy and dignity in cases involving cyber harassment. The misuse of personal information, unauthorised access to private accounts and non-consensual sharing of private images can seriously interfere with a woman's personal privacy. The section examines how digital technology has created new challenges for protecting private information and personal identity. It also considers the importance of consent, control over personal information and protection against the unnecessary exposure of private life. The connection between privacy, dignity and cyber harassment is important for assessing the adequacy of existing legal protection.

4.5 Underreporting and Lack of Cyber Awareness

This section examines the practical reasons why many incidents of cyber harassment may not be reported to the authorities. Women may avoid reporting because of lack of awareness about cyber laws, fear of social judgment, embarrassment, threats from offenders or lack of confidence in the complaint process. The section also considers the importance of legal and cyber awareness in enabling women to recognise online offences and seek appropriate remedies. The existence of legal provisions alone may not provide effective protection if victims are unaware of their rights or do not know where and how to report the offence.

4.6 Anonymity and Identification of Offenders

Anonymity is one of the major challenges in dealing with cyber harassment. Offenders may use fake accounts, false identities, temporary accounts or other methods to hide their identity. This can make it difficult for investigating authorities to identify the actual person responsible for the harassment. This section examines the difficulties involved in tracing offenders and obtaining relevant information from digital platforms. It also considers how anonymity can affect investigation and prosecution and why effective cooperation between law enforcement authorities and digital platforms is necessary.

4.7 Electronic Evidence and Jurisdictional Challenges

This section examines the practical difficulties involved in collecting and using electronic evidence in cyber harassment cases. Messages, screenshots, emails, social media posts,

photographs, videos and account information may be important for establishing the occurrence of an offence. However, digital evidence can be deleted, altered or difficult to obtain within a short period. The section also examines jurisdictional issues because cyber harassment may involve offenders, victims, digital platforms and electronic data located in different places. This can create difficulties in determining the appropriate authority and court for investigation and proceedings. These issues directly relate to the research gap concerning electronic evidence and jurisdiction.

4.8 Delays in Investigation and Prosecution

This section examines delays that may occur during the investigation and prosecution of cyber harassment cases. Delays may arise because of difficulties in identifying offenders, collecting electronic evidence, obtaining information from digital platforms and coordinating between different authorities. Such delays can reduce the effectiveness of legal remedies and may cause additional stress to victims. The section therefore considers the need for timely investigation, proper handling of electronic evidence and effective institutional coordination to ensure that women receive meaningful and timely protection.

This chapter shows that cyber harassment can seriously affect women's constitutional rights, particularly equality, freedom of expression, privacy and dignity. It also highlights practical difficulties such as underreporting, lack of awareness, anonymity, electronic evidence, jurisdiction and delay in investigation and prosecution. These issues show that the existence of legal provisions alone is not sufficient and that effective implementation and institutional support are necessary for better protection of women.

CHAPTER V – CRITICAL ANALYSIS, FINDINGS AND SUGGESTIONS

This chapter critically analyses the effectiveness of the existing legal and institutional framework for protecting women against cyber harassment in India. It examines the gaps in existing laws, the adequacy of protection available to women and the role of digital platforms. It also considers selected international approaches and presents the major findings and suggestions of the study. The chapter aims to identify the areas where legal and institutional measures can be improved to provide more effective protection to women in the digital environment.

5.1 Effectiveness of the Existing Legal Framework

This section critically examines whether the existing Indian legal framework provides effective protection to women against cyber harassment. The discussion in the previous chapters regarding the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023 will be considered together to assess their practical effectiveness. The section considers whether these laws are capable of dealing with the different and changing forms of cyber harassment identified in the study. It also examines whether the available legal remedies are accessible, timely and capable of providing meaningful protection to women. The difference between having legal provisions and effectively implementing them in practice will also be considered.

5.2 Gaps in Existing Cyber Laws

This section identifies the major gaps and limitations in the existing legal framework relating to cyber harassment against women. Although Indian law provides provisions that can be applied to several forms of online abuse, technological developments continue to create new methods of harassment. The section examines areas where the existing legal framework may require greater clarity or stronger implementation, particularly in relation to emerging forms of online harassment, anonymous offenders, misuse of digital platforms and removal of harmful content. It also considers whether the present legal framework is sufficiently flexible to respond to future developments in technology.

5.3 Adequacy of Protection Available to Women

This section evaluates whether the protection available to women is adequate from the legal and practical perspectives. Protection cannot be measured only by the existence of criminal provisions; it also depends on awareness, accessible reporting mechanisms, effective investigation, proper handling of electronic evidence and timely remedies. The section therefore examines whether women are able to make effective use of the available legal remedies when they face cyber harassment. It also considers the difficulties identified in the study, including underreporting, lack of cyber awareness, fear of social consequences, delay and difficulties in identifying offenders.

5.4 Role and Accountability of Digital Platforms

This section critically examines the role of social media platforms, messaging services and other digital intermediaries in preventing and responding to cyber harassment. Digital

platforms can assist victims through effective complaint mechanisms, timely removal or restriction of unlawful content and cooperation with investigating authorities. At the same time, the section considers the limits of platform responsibility and the need to balance user protection with freedom of expression. It examines whether existing mechanisms are sufficient to deal with repeated harassment, fake accounts and the circulation of private content and whether greater accountability is required from digital platforms.

5.5 Comparative International Perspective

This section provides a brief comparison between the Indian approach and selected international approaches to dealing with online harassment against women. It considers how other legal systems address issues such as online abuse, privacy violations, platform responsibility, reporting mechanisms and protection of victims. The purpose of the comparison is not to adopt foreign laws directly but to identify useful approaches that may strengthen the Indian legal and institutional framework. The comparative discussion will help in developing practical suggestions suitable to the Indian context.

5.6 Major Findings

This section presents the major findings that emerge from the doctrinal and analytical examination undertaken in the study. The findings will be based on the analysis of the forms of cyber harassment, existing laws, judicial decisions, constitutional rights and practical challenges discussed in the earlier chapters. The findings will particularly address whether the existing legal framework is sufficient, what difficulties women face in obtaining protection and how issues such as electronic evidence, anonymity, jurisdiction, digital platforms and delays affect the effectiveness of remedies. The findings will be presented in a clear manner and directly connected with the research objectives and questions.

5.7 Suggestions and Recommendations

Based on the findings of the study, this section provides suitable legal and institutional suggestions for improving protection against cyber harassment. The recommendations may include strengthening cyber awareness among women, improving reporting and complaint mechanisms, ensuring timely investigation, developing better methods for handling electronic evidence and improving coordination between law enforcement authorities and digital platforms. The section may also suggest greater accountability and effective response mechanisms for digital platforms and measures to deal with anonymous offenders and

emerging forms of cyber harassment. The suggestions will be framed with the aim of making existing protection more accessible, effective and responsive to the changing digital environment.

5.8 Conclusion

Cyber harassment against women has emerged as an important legal issue with the rapid expansion of the internet, social media and digital communication. The present study examined the nature and different forms of cyber harassment against women in India, including cyber stalking, online threats, impersonation, identity theft, fake accounts, abusive communication and the non-consensual sharing of private content. These forms of harassment may affect the privacy, dignity, reputation, personal safety and freedom of women in the digital environment. The study examined the existing Indian legal framework relating to cyber harassment through the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023. The Information Technology Act provides important provisions dealing with identity theft, cheating by personation, violation of privacy and certain forms of obscene or sexually explicit electronic content. The Bharatiya Nyaya Sanhita, 2023 further provides relevant offences relating to sexual harassment, voyeurism, stalking and acts intended to insult the modesty of women. The Bharatiya Sakshya Adhiniyam, 2023 is significant because electronic and digital records constitute an important part of cybercrime investigation and prosecution. The study also examined the constitutional dimension of cyber harassment. The rights guaranteed under Articles 14, 19 and 21 of the Constitution of India provide an important framework for understanding the impact of online harassment on equality, freedom of expression, privacy, dignity and personal liberty. The recognition of privacy as a constitutionally protected right in *Justice K.S.*

Puttaswamy (Retd.) v. Union of India has particular relevance to the protection of individuals against misuse of personal information and private digital content. Similarly, the decision in *Shreya Singhal v. Union of India* demonstrates the need to maintain a balance between protection from online abuse and the constitutional protection of freedom of speech and expression. The judicial decisions examined in this study also show that Indian courts have addressed different aspects of cyber offences, intermediary responsibility, privacy and protection of victims. The cases of *State of Tamil Nadu v. Suhas Katti*, *Avnish Bajaj v. State (NCT of Delhi)*, *Sharat Babu Digumarti v. Government of NCT of Delhi*, *Sabu Mathew George v. Union of India* and *Nipun Saxena v. Union of India* provide important judicial perspectives relevant to the development of cyber law and protection of individuals from online harm.

However, the study indicates that the existence of legal provisions alone does not completely resolve the practical difficulties faced by women. Cyber harassment frequently involves anonymous or pseudonymous accounts, rapidly changing digital platforms, cross-border elements, difficulties in preserving electronic evidence and delays in investigation. Victims may also face hesitation in reporting because of social pressure, fear of reputational harm, lack of awareness or concern about further harassment. Therefore, effective protection requires not only appropriate legislation but also accessible reporting mechanisms, trained investigating officers, effective digital forensic facilities and timely legal remedies. The responsibility of digital platforms is another important aspect identified by the study.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 prescribe due-diligence and grievance-redressal obligations for intermediaries. Effective implementation of these obligations is particularly relevant where harmful content, impersonation, threats or private material is circulated online. At the same time, platform regulation must operate consistently with constitutional principles and applicable law. The study further finds that electronic evidence has become central to the investigation and prosecution of cyber harassment. Screenshots, messages, emails, URLs, account information, metadata and other digital records may become important evidence depending upon the facts of a case. Proper preservation, collection, authentication and presentation of such evidence are therefore essential. The effectiveness of the legal framework depends substantially upon the ability of investigating agencies and courts to deal with technological evidence in a legally reliable manner. Cyber harassment is therefore not merely a technological problem but a legal, constitutional and institutional issue. The changing nature of technology requires continuous improvement in legal awareness, investigation methods, digital evidence practices and institutional responses. Women should be provided with accessible mechanisms for reporting cyber offences and obtaining timely assistance. Greater awareness of cyber safety and legal remedies is also necessary so that victims are able to respond to online harassment at an early stage. India has developed a substantial legal framework capable of addressing several forms of cyber harassment against women. Nevertheless, the effectiveness of this framework depends upon proper implementation, technological capacity, awareness, inter-agency coordination and timely access to justice. A balanced approach is therefore necessary—one that protects women from online harassment while also respecting privacy, dignity, equality and freedom of expression. Continuous legal and institutional development will remain necessary as new forms of digital harassment emerge with technological advancement.

REFERENCES

BOOKS

1. Debarati Halder & K. Jaishankar
2. Pavan Duggal
3. Avneet Kaur

STATUTES

1. Constitution of India, 1950
2. Information Technology Act, 2000
3. Bharatiya Nyaya Sanhita, 2023
4. Bharatiya Sakshya Adhiniyam, 2023
5. IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

ONLINE SOURCES

1. <https://www.indiacode.nic.in/>
2. <https://www.meity.gov.in/>
3. <https://www.cybercrime.gov.in/>
4. <https://www.sci.gov.in/>

WHITE BLACK
LEGAL