

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

**“Join the League of
National & International Scholars”**



EDITORIAL TEAM

DR. AJAY BHUPENDRA JAISWAL

Professor & Former Head
Department of Law
V.S.S.D. College, Nawabganj,
(C.S.J.M. University, Kanpur)

DR. MEGHA OJHA

Associate Professor | Legal Consultant
| Author | KLEF College of Law

PROF. DR. DEEVANSHU SHRIVASTAVA

Founding Dean and Professor,
GL Bajaj Institute of Law,
Greater Noida

DR. GAURAV GUPTA

Assistant Professor,
Faculty of Law, Lucknow

MR. TUHIN MUKHARJEE

Leadership Strategist | Business Coach
| Author | Speaker

MR. PRAKARSH PANDEY

Author and
Advocate, Allahabad High Court

MR. AMARESH PATEL

Assistant Professor
at Law School,
Amity University, Patna



LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

Copyright © 2025, LexScripta

ISSN-2583-8725

Vol - IV, Issue - I

Published by INTEGRITY EDUCATION INDIA

New Delhi

First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002

Phone: +91 98 11 66 62 16 (M)

Phone: +91 70 11 60 56 18 (M)

Bengaluru

Jallahalli East

Bengaluru, Karnataka. India.

Phone: +91 98 11 66 62 16 (M)

Email: publisher.integrity@gmail.com

USA

New Jersey

14 Grandview Ave, Upper Saddle River,

NJ-07458, USA

Phone: +14805226504 (M)

London

37 Degree Media

64, Hodder Drive, Perivale, London UB68LL.

United Kingdom.

Phone: +44 7950 78 18 17 (M)

Website: integrityeducation.co.in

© Lex Scripta Magazine Of Law And Policy, 2025

Disclaimer

All Copyrights are reserved with the Authors. But, however, the Authors have granted to the Journal (Lex Scripta Magazine of Law and Policy), an irrevocable, non-exclusive, royalty-free and transferable license to publish, reproduce, store, transmit, display and distribute it in the Journal or books or in any form and all other media, retrieval systems and other formats now or hereafter known. No part of this publication may be reproduced, stored, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

The Editorial Team of Lex Scripta Magazine of Law and Policy Issues holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not necessarily reflect the views of the Editorial Team of Lex Scripta Magazine of Law and Policy.

[© Lex Scripta Magazine of Law and Policy. Any unauthorized use, circulation or reproduction shall attract suitable action under application law.]

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

**"Join the League of National
and International Scholars"**



Lex Scripta Journal

Online Misogyny and Gender-Based Cyber Violence in India: A Critical Socio-Legal Study

Authors

Komal

Dr. Cheena Abrol



Online Misogyny and Gender-Based Cyber Violence in India: A Critical Socio-Legal Study

Komal

*LL.M. Criminal Law
CT University Ludhiana*

Dr. Cheena Abrol

CT University, Ludhiana

Abstract

Digital platforms have grown quickly, which has changed how people talk to each other. But this has also made it easier for hate speech against women and cyber violence based on gender (GBCV) to spread online. Algorithms make things like cyberstalking, sexual harassment, doxxing, sharing pictures without permission, and hate speech worse. This can be especially bad for women and gender minorities. These kinds of abuse don't just happen once in the digital world; they show that patriarchal systems are still in place in virtual spaces. This paper examines online misogyny and gender-based cyber violence (GBCV) from a socio-legal perspective. It examines the interplay of social norms, technological infrastructures, and prevailing legal frameworks in influencing the nature of harm inflicted and the experiences of victims.

The research examines statutory provisions, judicial rulings, socio-legal scholarship, and empirical evidence to evaluate the adequacy of current legal responses. It raises significant issues, including jurisdictional challenges, insufficient reporting, inadequate enforcement of gender-sensitive legislation, and the tension between free speech and harm prevention. The paper examines the psychological, social, and democratic ramifications of digital gender violence, emphasizing its deterrent effect on women's public engagement.

The research indicates that punitive legal measures are insufficient in isolation; they must be integrated with platform accountability, algorithmic transparency, and institutional gender sensitivity. It ends by suggesting a complete plan that includes changes to the law, more oversight of middlemen, solutions that put victims first, and programs to help people learn how to use technology better. We need not only stronger cyber laws, but also to change the social and cultural conditions that let people be rude to women online.

Introduction

The digital revolution has changed a lot about how people get along, vote, do business, and talk to each other. It's easier than ever to talk to people and share your thoughts on social media, online forums, and messaging apps. There has been more online violence and hate against women, which is not good. Digital spaces were supposed to be places where everyone could take part equally, but they are becoming more and more like and even worse than the gender hierarchies and unfair treatment that happen in real life. Women and gender minorities often have to deal with hostility that isn't just a one-time thing; it's part of how online spaces are set up and run.¹

¹ Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).

People who are rude, hostile, or biased against women and gender minorities online are engaging in misogyny. It can happen in hate speech that is sexist, sexualized abuse, stereotypes that make women look less credible or independent, coordinated harassment campaigns, and stories that make women look less credible or independent. Misogynistic content is different from other kinds of online abuse because it is based on ideas that want to control, silence, or punish women for being in public places, whether they are political, professional, or personal. It often targets women who speak out, get involved in activism, or question how things are done in society.² Digital platforms make this kind of hate worse because they let people hide who they are, spread quickly, and be quick. This makes it easy for people to lie and plan group harassment without getting caught.

This is a lot like the idea of gender-based cyber violence (GBCV). Cyber violence based on gender is when people use technology to hurt, help, or make things worse for other people just because they are male or female. It includes planned trolling, online stalking, sexual harassment, sharing private photos without permission (often called "revenge pornography"), doxxing, morphing images, deepfake pornography, threats of sexual violence, and more. GBCV isn't just talk; it can really hurt people's health, money, reputation, and bodies. It is important to remember that these actions are often just more violence against women in real life. This shows how harm in the real world and online are connected.³

Hate speech and violence against women online are bad for the law and for society. Digital gender violence makes it harder for women to have the same chances as men in their personal and professional lives. Studies show that long-term online harassment can make people stop using social media, censor themselves, and have negative effects on their mental health, like anxiety, depression, and trauma.⁴ Women who work in politics, journalism, law, or as public servants are more likely to be in danger. The "chilling effect" that happens as a result goes against democratic values because it makes public debate less diverse and silences voices that are already weak.⁵

The law hasn't been able to keep up with how quickly technology changes. Today, most cybercrime laws are about things like harassment, defamation, and obscenity. But they don't really get how online abuse affects men and women in different ways. It's hard to enforce the law because of issues with jurisdiction, criminals' anonymity, gathering evidence, and the fact that law enforcement agencies aren't very good with technology. Regulators have a harder time doing their jobs when they have to protect free speech and keep bad content in check at the same time. Constitutional democracies protect free speech, but using this protection to defend hate speech against women is a big doctrinal problem.

The goal of this paper is to look at online hate against women and gender-based cyber violence from both a social and a legal point of view. It doesn't see digital abuse as a separate crime; instead, it sees it as part of a larger pattern of unfairness and social norms that affect both behavior and how institutions react.⁶

² UN Women, *Online and ICT-facilitated Violence against Women and Girls during COVID-19* (2020).

³ Amnesty International, *Toxic Twitter: Violence and Abuse against Women Online* (2018).

⁴ Plan International, *Free to Be Online? Girls' and Young Women's Experiences of Online Harassment* (2020).

⁵ Council of Europe, *Mapping the Study on Cyberviolence* (2018).

⁶ Jane Bailey & Valerie Steeves, "eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices," (2015) 33 *Canadian Journal of Law & Society* 1.

Theoretical And Conceptual Framework

We need to look at more than just the law to understand how women are treated badly online and how men are treated badly online. We need to use a lot of different theories to explain how gendered power structures work online. This part of the study looks at the phenomenon in the context of feminist legal theory, the public-private divide, cyberfeminism, and structural theories of patriarchy. This study exemplifies interdisciplinary research.⁷

2.1 Feminist Legal Theory and Structural Inequality

Feminist legal theory contests the idea that the law is fair and unbiased. It says that patriarchal norms have shaped legal systems throughout history by putting men's experiences ahead of women's and pushing women's realities to the side. The idea of substantive equality by Catharine MacKinnon is very useful.⁸ Formal equality says that men and women are equal, while substantive equality looks at whether different legal responses are needed for structural disadvantages.

Online misogyny shows that digital spaces that seem fair can make things worse for everyone. Laws against harassment and obscenity don't always look at the gendered patterns that lead to abuse. The law calls hate speech online "offensive content," which makes it hard to see how women are treated unfairly when they are attacked. Feminist legal theory advocates for a transition from an individualistic perspective on harm to a structural analysis. Digital harassment is a way for society to keep people in line, which is why this happens.⁹

Feminist jurisprudence illustrates the utilization of sexual abuse as a means of control over individuals. There are a lot of threats of rape, sexual humiliation, and sending pictures without permission. This shows how people try to control women who don't fit into the roles that society wants them to play. People don't fully understand what harm is because the law doesn't make it clear that this is violence against women.¹⁰

2.2 Patriarchy in Digital Spaces

Women are not in charge most of the time in a society where men are. It also exists in digital spaces, like the way platforms are made, the cultures of the people who use them, and the way algorithms make things more popular. Online spaces aren't just neutral tech. They're socio-technical systems that are shaped by cultural biases and economic incentives.¹¹

People can often do things on digital platforms without having to answer for them. It's easy for people to work together to annoy other people without worrying about getting in trouble. Also, algorithms that are based on engagement give more weight to content that is controversial and makes people feel strongly. This means that stories that are sexist become more popular, even if they don't mean to. This structural feature turns single acts of abuse into patterns of hostility

⁷ UN Human Rights Council, *Report of the Special Rapporteur on Violence against Women, its Causes and Consequences on Online Violence against Women and Girls A/HRC/38/47* (2018).

⁸ Asia Pacific Forum on Women, Law and Development (APWLD), *Technology-Facilitated Gender-Based Violence in Asia* (2021).

⁹ Danielle Keats Citron & Mary Anne Franks, "Criminalizing Revenge Porn," (2014) 49 *Wake Forest Law Review* 345.

¹⁰ Clare McGlynn, Erika Rackley & Ruth Houghton, "Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse," (2017) 25 *Feminist Legal Studies* 25.

¹¹ United Nations General Assembly, *Convention on the Elimination of All Forms of Discrimination against Women* (CEDAW), 1979.

that affect the whole system.¹² Digital misogyny often happens when women enter fields that have mostly been male-dominated in the past, such as politics, law, gaming, or technology. The backlash against women in public life shows that men can use digital tools to get their power back. The internet doesn't always make it easier for everyone to get involved; in fact, it often shows how people are different in real life.

2.3 The Public–Private Divide

The traditional legal distinction between public and private spheres has historically limited state intervention in matters deemed "private," including domestic violence and sexual harassment. Feminist scholars have long argued that this separation obscures systemic issues by making violence against women invisible to public scrutiny.¹³

The line between public and private gets blurrier in digital spaces. People all over the world can see posts on social media, even if they look private. People can post pictures of two people they know without asking them first. Cyberstalkers often go too far by sending messages and keeping an eye on people all the time.

This is a tough line for the law to draw. For instance, most people don't think it's okay to share private pictures without permission. The harm is very personal, but the effect is very public. "The personal is political" is a very important idea when it comes to online gender violence because anyone can be a victim of digital abuse.¹⁴

2.4 Cyberfeminism and Digital Agency

Cyberfeminism emerged as a movement that examines the emancipatory potential of digital technologies for women. Early cyberfeminism theory viewed the internet as a medium for individuals to transform their identities and dismantle social hierarchies. Things are harder now than they were before, though. Digital platforms like #MeToo have made it easier for feminists to work together, protest, and help each other.¹⁵ But they have also turned into places where people are more likely to fight back. The same technologies that let women speak out against things also make it easier for people to plan to hurt their reputations and bother them.

Cyberfeminism research is currently examining the dual nature of digital environments as both liberating and oppressive. But they aren't places where different types of power are at war with each other. A socio-legal framework must address both empowerment and vulnerability concerning the utilization of digital technology.¹⁶

2.5 Technology-Facilitated Violence as a Continuum

The "continuum of violence" is a feminist criminology concept that posits various forms of gender-based harm are interconnected rather than isolated. This range includes threats, verbal abuse, image-based abuse, physical violence, and online misogyny. Research indicates that online threats frequently escalate into stalking or physical violence. People who have been hurt by violence have mental problems that are similar to those of other types of violence, even if

¹² Apar Gupta & Faizan Mustafa, "The Right to Freedom of Speech and Expression in the Age of Social Media," (2016) 8 *NUJS Law Review* 1.

¹³ Carole Pateman, *The Sexual Contract* (Stanford University Press, 1988).

¹⁴ Catharine A. MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press, 1989).

¹⁵ Kimberlé Crenshaw, "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color," (1991) 43 *Stanford Law Review* 1241.

¹⁶ United Nations General Assembly, *Declaration on the Elimination of Violence against Women*, 1993.

they weren't physically hurt. It's harder to say that digital abuse isn't real or important when you know that this continuum exists.

When you say that cyber harassment isn't as bad as physical violence, it makes things worse for the people who have been hurt. A continuum framework helps regulators step in and find solutions that put the needs of victims first.¹⁷

2.6 Free Speech and Harm: A Normative Tension

Finding the right balance between free speech and keeping people safe is one of the hardest parts of stopping online misogyny. Liberal constitutional traditions underscore the importance of free speech in a democratic society. Feminist scholars assert that unregulated hate speech oppresses marginalized groups, thus obstructing substantive democratic participation.¹⁸ The conversation is about whether saying hateful things about women is protected speech or bad behavior. Courts don't all agree on what hate speech laws should be. Some courts are very strict about what people can say, as long as it doesn't cause violence. Other courts are more open to hate speech laws.

A socio-legal framework must exercise considerable caution in addressing this tension. It shouldn't censor too much, but it should also know that women don't talk to each other online because they are always being harassed. When hate speech based on gender clearly harms individuals, substantive equality may necessitate specific regulation of it.¹⁹

2.7 Platform Governance and Algorithmic Power

Most digital spaces are run by private companies, but traditional legal theory often looks at how the government controls things. The owners of social media sites decide how people can talk to each other, how they can control what people see, and how algorithms choose the best user.

People are worried about being held accountable, being honest, and getting due process because of this privatized government. There may not always be the same ways to moderate content, and automated systems might not be able to find small forms of sexism. Furthermore, the quest for profit often hinders the prevention of harm before it transpires.²⁰ A socio-legal analysis must examine more than merely the laws to assess a business's accountability. You need to know how state law and platform governance work together to understand how gender-based cyber violence is handled.

Forms of Online Misogyny and Gender-Based Cyber Violence

There are many different kinds of hate against women and gender-based cyber violence online, and they change over time. Even though technology changes, the basic ideas of humiliation, control, and exclusion stay the same. This section talks about the different types of digital gender violence, how they work, and why the laws we have now don't always work well with them.²¹

¹⁷ Anita Gurumurthy & Nandini Chami, "Digital Gender Divide and the Political Economy of ICTs," (2014) 49 *Economic and Political Weekly* 44.

¹⁸ Nancy Fraser, "Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy," (1990) 25 *Social Text* 56.

¹⁹ Tarana Burke, "Me Too Is a Movement, Not a Moment," (2018) *TEDWomen*.

²⁰ Association for Progressive Communications (APC), *Online Gender-Based Violence and Women's Human Rights* (2017).

²¹ Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019).

3.1 Cyber Harassment and Gendered Hate Speech

Cyber harassment is when someone keeps doing something mean or threatening to someone else online. This kind of harassment is a type of online misogyny if it is directed at people because of their gender. This includes body shaming, sexist insults, and threats of rape, as well as insults about women's looks, morals, or skills.²²

Organized trolling campaigns often use hate speech based on gender, which is different from insults that come from one person. People who work in the public eye, such as journalists, politicians, lawyers, activists, and academics, are more likely to be attacked. People who abuse others often make clear threats of sexual violence to hurt them and scare them into silence.

The most important thing that sets gendered cyber harassment apart is that it is sexual. Men in the public eye may get hate or criticism, but women are more likely to be attacked for their bodies, sexuality, or how people see them as a person. These patterns show that stereotypes about men, not random hate on the internet, are what hurt people.

This damage gets worse because it spreads so quickly on social media. One hateful post about women can be shared thousands of times, which makes it even more powerful and bad for the mind. Digital content lasts forever, so the damage is worse because abusive content can come back long after it was first posted.²³

3.2 Cyberstalking and Online Surveillance

When someone uses digital tools to watch, message, or follow someone else, that's called cyberstalking. People who do these things might send unwanted messages over and over, follow their victims' online activity, pretend to be them, or use spyware and location-based technologies to keep an eye on where they are.

Cyberstalking based on gender is like violence against women by their partners in real life. Ex-partners may use digital platforms to control, threaten to share private information, or scare victims. You can reach them by email, social media, and messaging apps, which makes it seem like they are always watching you.²⁴

The brain is very badly affected. People who have been hurt often say they are scared, worried, and on edge about getting hurt again. The idea of a continuum of harm is stronger because threats online and violence in the real world are so similar. People often stalk each other online before or while they are bothering each other in real life.

Because of problems with jurisdiction and evidence, the law has a harder time dealing with cyberstalking. It's hard to find and punish people because of anonymous accounts, encrypted messaging services, and platforms that work across borders.²⁵

3.3 Non-Consensual Dissemination of Intimate Images

Sharing private photos without a woman's permission is one of the worst kinds of cyber violence against women. People sometimes call it "revenge pornography," but that's not the right word because it sounds like revenge on a small scale instead of abuse on a larger scale.

²² Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010).

²³ Deborah L. Rhode, *The Beauty Bias* (Oxford University Press, 2010).

²⁴ Mary Anne Franks, *The Cult of the Constitution* (Stanford University Press, 2019).

²⁵ Martha C. Nussbaum, *Sex and Social Justice* (Oxford University Press, 1999).

People often use threats, hacking, or blackmail instead of revenge. These include sharing private photos or videos without permission, changing pictures to make them sexual, and using AI to make fake porn and share it. The goal is often to make the victim feel bad, scared, or want to stay away from them.

Sometimes the damage is so bad that you can't go to school or be seen in public. It can also hurt your mental health, your family, and your job. It's hard to get rid of digital content because it lasts forever and can be copied, even if it's legal. This is more likely to hurt women than men. Women who have sex are looked down upon more than men who do. When stories blame the victim, fewer people are likely to report the crime, and the stigma around it grows.²⁶

3.4 Doxxing and Identity-Based Intimidation

When someone shares private or personal information about someone else without their permission, this is called doxxing. This includes your address, phone number, work information, and information about your family. Doxxing is a way to scare women, especially famous ones.²⁷

When private information is made public, victims may get threatening phone calls, be harassed, or even hurt in real life. It also makes your coworkers and family members stressed out. The goal is often to punish women for saying things that make people disagree or to make people who disagree with them be quiet.

Doxxing is a good example of how being open online can put you in danger in the real world. The event takes place online, but it also has effects in the real world. A lot of women don't want to do things online because they're scared of getting hurt.

3.5 Impersonation and Identity Theft

Making fake accounts in someone else's name to spread lies or hurtful information is called online impersonation. People who do these things might use the victim's name to post porn or send rude messages to other people. This can damage their own and others' reputations.²⁸ Women who work as lawyers, teachers, or journalists can hurt their chances of getting a job and their reputation by pretending to be someone else. Even if someone deletes their accounts, their reputation could still be hurt. The impersonation is sexual, which is what makes it a gender. Fake accounts often show women in sexual or embarrassing situations, which makes sexist stereotypes stronger.²⁹

Legal Framework and Doctrinal Analysis

The regulation of online misogyny and gender-based cyber violence (GBCV) operates within the comprehensive constitutional and statutory framework that regulates speech, privacy, and criminal conduct. India has a lot of laws that stop digital abuse, but there isn't one set of rules that is sensitive to gender and deals specifically with violence against women that technology makes easier.

²⁶ Judith Butler, *Gender Trouble* (Routledge, 1990).

²⁷ Laura Bates, *Men Who Hate Women* (Simon & Schuster, 2020).

²⁸ Emma A. Jane, "Online Misogyny and Feminist Digilantism," (2017) 22 *Continuum* 284.

²⁹ Jeremy Waldron, *The Harm in Hate Speech* (Harvard University Press, 2012).

4.1 Constitutional Context: Free Speech and Dignity

*Article 19(1)(a)*³⁰ of the Indian Constitution guarantees freedom of speech and expression. However, *Article 19(2)*³¹ permits reasonable restrictions in the interests of public order, decency, morality, defamation, and incitement to an offence. The constitutional tension arises when misogynistic or abusive online speech is defended as protected expression.

In *Shreya Singhal v. Union of India* (2015)³², the Supreme Court struck down Section 66A of the Information Technology Act, 2000, on grounds of vagueness and overbreadth. While the judgment strengthened digital free speech protections, it also removed a frequently used provision against online harassment. The Court clarified that only speech that amounts to incitement or falls within Article 19(2) restrictions can be penalized. Consequently, many forms of online misogyny that are abusive but do not meet the threshold of incitement remain difficult to regulate.

At the same time, *Article 21*³³ guarantees the right to life and personal liberty, which includes dignity and privacy. Gender-based cyber violence directly infringes these constitutional values, requiring a careful balance between free expression and protection from harm.

4.2 Information Technology Act, 2000

The IT Act forms the core statutory framework for cyber offences.

Section 66E³⁴ criminalizes violation of privacy through capturing or transmitting images of a private area without consent. This provision is relevant in cases of non-consensual sharing of intimate images but is limited to visual privacy and does not comprehensively address emerging harms such as deepfake pornography.

Sections 67 and 67A³⁵ penalize the publication or transmission of obscene or sexually explicit material in electronic form. These sections are frequently invoked in cases of image-based abuse. However, the legal framing focuses on obscenity rather than on the gendered harm inflicted upon victims. This approach risks reinforcing moralistic standards instead of recognizing the act as a form of violence and coercion.

The **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**³⁶ impose due diligence obligations on social media intermediaries, requiring removal of unlawful content and establishment of grievance redressal mechanisms. While these rules enhance platform accountability, enforcement remains inconsistent, and victims often face delays in content removal.

4.3 Indian Penal Code Provisions

Several provisions of the Indian Penal Code (IPC) supplement cyber-specific laws.

Section 354A³⁷ addresses sexual harassment and may extend to unwelcome sexual advances made through digital platforms.

³⁰ Constitution of India, 1950, Art. 19(1)(a).

³¹ Constitution of India, 1950, Art. 19(2).

³² *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

³³ Constitution of India, 1950, Art. 21.

³⁴ Information Technology Act, 2000, s. 66E.

³⁵ Information Technology Act, 2000, ss. 67 & 67A.

³⁶ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

³⁷ Indian Penal Code, 1860, s. 354A.

Section 354D³⁸ explicitly criminalizes stalking, including monitoring a woman's internet use or electronic communication, thereby recognizing cyberstalking as an offence.

Section 509³⁹ penalizes words or gestures intended to insult the modesty of a woman and is often used in cases involving obscene online comments. However, the language of "modesty" reflects a traditional and arguably outdated understanding of gender protection. Additionally,

Section 506⁴⁰ (criminal intimidation) may apply to online rape or death threats.

Despite the availability of these provisions, enforcement challenges persist. Anonymous accounts, cross-border platforms, evidentiary difficulties, and limited cyber forensic capacity hinder effective prosecution.

4.4 Comparative and International Perspectives

Globally, regulatory approaches are evolving. The United Kingdom's Online Safety Act imposes proactive duties on platforms to mitigate harmful content, including abuse targeting women and girls. Similarly, the *European Union's Digital Services Act*⁴¹ emphasizes algorithmic transparency and systemic risk management. International human rights instruments such as CEDAW⁴² obligate states to eliminate discrimination and exercise due diligence in addressing gender-based violence, including technology-facilitated harm. These frameworks recognize that digital violence forms part of a broader continuum of gender-based abuse.

Enforcement Challenges and Socio-Legal Gaps

Despite the existence of multiple statutory provisions addressing harassment, obscenity, stalking, and privacy violations, enforcement against online misogyny and gender-based cyber violence (GBCV) remains significantly inadequate.⁴³ The problem lies not merely in legislative gaps but in structural, procedural, and socio-cultural barriers that undermine effective implementation.⁴⁴

5.1 Underreporting and Social Stigma

One of the most persistent challenges is underreporting. Victims of online gender-based abuse frequently hesitate to approach law enforcement due to fear of social stigma, victim-blaming, and reputational damage. In societies where female sexuality is closely policed, survivors of image-based abuse or sexual harassment often face moral scrutiny rather than institutional support. This discourages complaints and perpetuates impunity.

Additionally, the normalization of online abuse particularly in political or professional contexts creates an environment where harassment is dismissed as "part of being online." Such trivialization minimizes the seriousness of digital violence and contributes to institutional inaction.⁴⁵

³⁸ Indian Penal Code, 1860, s. 354D.

³⁹ Indian Penal Code, 1860, s. 509.

⁴⁰ Indian Penal Code, 1860, s. 506.

⁴¹ European Union, *Digital Services Act*, Regulation (EU) 2022/2065.

⁴² Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979.

⁴³ UN Committee on the Elimination of Discrimination against Women, General Recommendation No. 35 on Gender-Based Violence against Women (2017).

⁴⁴ Susan Herring, "Gender and Power in Online Communication," (1996) 3 *The Information Society* 129.

⁴⁵ Alexander Brown, *Hate Speech Law: A Philosophical Examination* (Routledge, 2015).

5.2 Anonymity and Jurisdictional Barriers

Digital platforms enable anonymity and pseudonymity, complicating identification of perpetrators. Fake accounts, encrypted messaging services, and virtual private networks (VPNs) obscure digital footprints. Even where identities are traceable, platforms may be headquartered abroad, creating jurisdictional hurdles. Cross-border data access requires cooperation through mutual legal assistance treaties (MLATs), which are often time-consuming. In cases of viral abuse, delays in obtaining data may result in loss of evidence or continued dissemination of harmful content. The global nature of digital platforms challenges traditional territorial models of criminal jurisdiction.⁴⁶

5.3 Evidentiary and Procedural Limitations

Successful prosecution of cyber offences requires technical expertise in digital forensics. However, law enforcement agencies often lack adequate infrastructure and specialized training. Improper evidence collection may render digital proof inadmissible or unreliable. Furthermore, procedural delays within the criminal justice system exacerbate trauma for victims. Lengthy investigations and trials discourage sustained engagement with legal processes. Interim relief mechanisms, such as immediate content takedown or restraining orders, are not always accessible or effective.⁴⁷

Critical Analysis and Reform Recommendations

The preceding analysis demonstrates that while legal provisions addressing online harassment and cybercrime exist, they remain fragmented, reactive, and insufficiently attuned to the structural nature of gender-based digital harm. A critical socio-legal evaluation reveals that addressing online misogyny requires more than criminalization; it demands systemic reform integrating constitutional values, technological accountability, and gender-sensitive governance.⁴⁸

6.1 Beyond Fragmentation: Toward a Coherent Legal Framework

Indian law currently addresses online misogyny through scattered provisions under the Information Technology Act and the Indian Penal Code. This fragmented approach treats offences as isolated acts of obscenity, defamation, or stalking rather than as manifestations of gender-based violence. A more coherent statutory framework should explicitly recognize technology-facilitated gender violence as a distinct category of harm.⁴⁹

Legislative reform could consolidate provisions relating to cyberstalking, image-based abuse, deepfakes, and digital harassment into a comprehensive statute or introduce targeted amendments that clearly define gender-based cyber violence. Explicit recognition would improve doctrinal clarity, enhance reporting, and promote victim-centered interpretation.

6.2 Gender-Sensitive Interpretation and Substantive Equality

Formal equality treating all individuals identically under gender-neutral laws does not sufficiently address the disproportionate impact of online abuse on women. Courts and enforcement authorities must adopt a substantive equality approach grounded in Articles 14 and 21 of the Constitution.⁵⁰

⁴⁶ Tarleton Gillespie, *Custodians of the Internet* (Yale University Press, 2018).

⁴⁷ Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech," (2018) 131 *Harvard Law Review* 1598.

⁴⁸ Jack Balkin, "Free Speech in the Algorithmic Society," (2018) 51 *UC Davis Law Review* 1149.

⁴⁹ Frank Pasquale, *The Black Box Society* (Harvard University Press, 2015).

⁵⁰ Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999).

Judicial interpretation should acknowledge that persistent digital harassment undermines dignity, privacy, and equal participation in public life. Recognizing online misogyny as discriminatory conduct rather than mere offensive speech would enable more balanced constitutional reasoning. Such an approach would not dilute free speech protections but would contextualize them within the broader framework of equality and human dignity.⁵¹

6.3 Strengthening Platform Accountability

Given that digital platforms function as primary spaces of public discourse, regulatory reform must extend beyond criminal liability of individuals. Platforms should be required to implement:

- Transparent and accessible grievance redressal mechanisms
- Time-bound takedown procedures for image-based abuse
- Algorithmic transparency and risk assessment for amplification of harmful content
- Stronger identity verification mechanisms in cases involving repeated abuse⁵²

However, regulation must avoid excessive state control over digital speech. Independent oversight bodies or co-regulatory models involving civil society participation may provide a balanced approach.

6.4 Addressing Emerging Technologies

The rapid growth of artificial intelligence tools, including deepfake generation, necessitates proactive legislative measures. Laws must explicitly criminalize the creation and dissemination of synthetic sexually explicit content without consent, regardless of whether original images were captured. Preventive mechanisms, including watermarking technologies and AI detection tools, should be integrated into regulatory frameworks.

Failure to anticipate technological innovation will perpetuate reactive lawmaking, leaving victims unprotected until harm becomes widespread.⁵³

Conclusion

The expansion of digital technologies has reshaped contemporary social, political, and economic life, positioning online platforms as central arenas of public discourse. Yet, as this study demonstrates, these digital spaces have also become sites where entrenched gender hierarchies are reproduced and intensified.⁵⁴ Online misogyny and gender-based cyber violence are not incidental by-products of technological growth; they are structural manifestations of broader social inequalities embedded within digital ecosystems.⁵⁵

This paper has examined the phenomenon through a socio-legal lens, highlighting how online harassment, cyberstalking, non-consensual dissemination of intimate images, doxxing, and emerging harms such as deepfake pornography collectively form part of a continuum of gender-based violence. These practices function not merely to offend but to intimidate, silence, and exclude women from equal participation in digital public life. The chilling effect on speech, professional engagement, and political involvement undermines democratic values and constitutional commitments to equality.

⁵¹ United Nations Human Rights Council, *The Right to Privacy in the Digital Age*, A/HRC/RES/34/7 (2017).

⁵² Special Rapporteur on Freedom of Expression, *Report on Online Hate and Disinformation*, A/74/486 (2019).

⁵³ UN Broadband Commission for Sustainable Development, *Cyber Violence against Women and Girls: A Worldwide Wake-Up Call* (2015).

⁵⁴ Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton University Press, 2017).

⁵⁵ Henry Jenkins, *Convergence Culture: Where Old and New Media Collide* (New York University Press, 2006).

The doctrinal analysis reveals that while Indian law provides multiple statutory avenues to address digital abuse, the existing framework remains fragmented and reactive. Provisions under the Information Technology Act and the Indian Penal Code conceptualize harm in terms of obscenity, defamation, or harassment, without explicitly recognizing the structural and gendered nature of the violence involved.⁵⁶ The constitutional commitment to free speech, reinforced by judicial decisions such as *Shreya Singhal v. Union of India*, has strengthened civil liberties but simultaneously exposed regulatory gaps in addressing gendered online abuse. The challenge, therefore, lies in harmonizing freedom of expression with the protection of dignity, privacy, and substantive equality under Articles 14 and 21.

Beyond legislative shortcomings, enforcement barriers including underreporting, social stigma, anonymity, jurisdictional constraints, and limited cyber forensic capacity significantly impede effective remedies. Platform governance further complicates accountability, as algorithmic amplification and profit-driven engagement models often enable the spread of misogynistic content. The privatization of digital regulation raises critical questions regarding transparency, due process, and corporate responsibility.⁵⁷ The future of digital democracy depends upon this balance.

References

A. Books

- Balkin, Jack, *Free Speech in the Algorithmic Society* (Yale University Press, 2018).
- Bates, Laura, *Men Who Hate Women* (Simon & Schuster, 2020).
- Bhatia, Gautam, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* (Oxford University Press, 2016).
- Citron, Danielle Keats, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).
- Franks, Mary Anne, *The Cult of the Constitution* (Stanford University Press, 2019).
- Gillespie, Tarleton, *Custodians of the Internet* (Yale University Press, 2018).
- Lessig, Lawrence, *Code and Other Laws of Cyberspace* (Basic Books, 1999).
- MacKinnon, Catharine A., *Toward a Feminist Theory of the State* (Harvard University Press, 1989).
- Menon, Nivedita, *Seeing Like a Feminist* (Zubaan, 2012).
- Nissenbaum, Helen, *Privacy in Context* (Stanford University Press, 2010).
- Noble, Safiya Umoja, *Algorithms of Oppression* (New York University Press, 2018).
- Nussbaum, Martha C., *Sex and Social Justice* (Oxford University Press, 1999).
- Pasquale, Frank, *The Black Box Society* (Harvard University Press, 2015).
- Pateman, Carole, *The Sexual Contract* (Stanford University Press, 1988).
- Plant, Sadie, *Zeros + Ones* (Fourth Estate, 1997).
- Sunstein, Cass R., *#Republic: Divided Democracy in the Age of Social Media* (Princeton University Press, 2017).
- Wajcman, Judy, *TechnoFeminism* (Polity Press, 2004).
- Zuboff, Shoshana, *The Age of Surveillance Capitalism* (PublicAffairs, 2019).

⁵⁶ Law Commission of India, Report No. 273, *Implementation of 'United Nations Convention against Torture' and Other Cruel, Inhuman and Degrading Treatment or Punishment* (2017).

⁵⁷ UN Special Rapporteur on Violence against Women, *Online Violence against Women and Girls from a Human Rights Perspective*, A/76/142 (2021).

B. Articles

- Brown, Alexander, "Hate Speech Law: A Philosophical Examination," (2015) *Routledge*.
- Citron, Danielle Keats & Franks, Mary Anne, "Criminalizing Revenge Porn," (2014) 49 *Wake Forest Law Review* 345.
- Crenshaw, Kimberlé, "Mapping the Margins," (1991) 43 *Stanford Law Review* 1241.
- Fraser, Nancy, "Rethinking the Public Sphere," (1990) 25 *Social Text* 56.
- Herring, Susan, "Gender and Power in Online Communication," (1996) 3 *The Information Society* 129.
- Jane, Emma A., "Online Misogyny and Feminist Digilantism," (2017) 22 *Continuum* 284.
- Klonick, Kate, "The New Governors," (2018) 131 *Harvard Law Review* 1598.
- McGlynn, Clare & Rackley, Erika, "Image-Based Sexual Abuse," (2017) 37 *Oxford Journal of Legal Studies* 534.

C. Cases

- *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.
- *Indian Young Lawyers Association v. State of Kerala*, (2019) 11 SCC 1.
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
- *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221.
- *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241.

D. Legislation

- Constitution of India, 1950.
- Indian Penal Code, 1860.
- Information Technology Act, 2000.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- Protection of Women from Domestic Violence Act, 2005.
- United Kingdom, *Online Safety Act*, 2023.
- European Union, *Digital Services Act*, Regulation (EU) 2022/2065.

E. Reports & International Instruments

- Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979.
- Law Commission of India, Report No. 267, *Hate Speech* (2017).
- OECD, *Bridging the Digital Gender Divide* (2018).
- UN Broadband Commission for Sustainable Development, *Cyber Violence against Women and Girls* (2015).
- UN Committee on the Elimination of Discrimination against Women, General Recommendation No. 35 (2017).
- UN Human Rights Council, *The Right to Privacy in the Digital Age* (2017).
- UN Special Rapporteur on Violence against Women, *Online Violence against Women and Girls* (2021).
- World Wide Web Foundation, *Women's Rights Online Report* (2020).

EDITORIAL TEAM

PROF. (DR.) BANSHI DHAR SINGH

Professor,
Ex. Dean & Head,
Faculty of Law,
University of Lucknow

DR. KALPESHKUMAR L GUPTA

Founder ProBono India, Legal Start-ups,
Law Teachers India

DR. SUDHANSHU CHANDRA

Assistant Professor, Manuu Law
School, Maulana Azad National Urdu
University (Central University),
Hyderabad

PROF. (DR.) SANJAY SINGH

Director
of IIMT College of Law

INTERNATIONAL EDITORIAL TEAM

PROF. DR. MARC OLIVER OPRESNIK

President and CEO
Opresnik Management Consulting
and Opresnik Business School

**PROF. DR. COMRADE AMB.
CHUKWUNONSO C
HARLES OFODUM ESQ**

Chancellor, ALSA University.
Legal Director for Nigeria, World
Association for Humanitarian Doctors

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- | **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- | **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- | **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- | **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- | **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.



CONNECT WITH US **9811 666 216**
7011 605 618

