INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

"VICTIMOLOGY: A BRANCH OF CRIMINOLOGY"

AUTHORED BY – ANSHIKA SINGH
BBA.LLB (H), 2nd year (Amity Law School)

CO-AUTHOR - DR. ARVIND KUMAR SINGH
Associate Professor (ALS)
Amity University Uttar Pradesh, Lucknow

ABSTRACT

India's rapid digital boom has completely changed how gender-based violence shows up—it's moved from physical spaces into the tough, tech-driven world of the internet. Cyber crimes against women—from stalking and sharing intimate images without consent, to deepfake porn, identity theft, and online fraud—are now common threats. They go after basic rights like privacy, dignity, equality, and free speech.

In this paper, I take a close look at the legal, structural, and social sides of these crimes. The main legal frameworks—the Information Technology Act (2000), the Indian Penal Code, and the Digital Personal Data Protection Act (2023)—offer some remedies, but these laws usually react after the fact and can't keep pace with how fast and anonymously cyber offences happen. Using NCRB data, court decisions, and human rights standards from around the world, I point out some major flaws: for instance, there's no specific law tackling new synthetic digital harms, it's tough to prove cases or find offenders across jurisdictions, and shame keeps many victims silent. I suggest a multi-layered solution with better laws, smarter tech, stronger institutions, and more public awareness. The bottom line? Cyber crimes against women aren't just "one-off" incidents—they're part of an ongoing pattern of gender inequality online, and we need a proactive, rights-focused approach to deal with them.

INTRODUCTION

As India moves toward becoming a digital powerhouse, how people connect with each other is changing really fast. Over 900 million people are online now, using popular platforms like Instagram, WhatsApp, and YouTube. These spaces are key for communication, jobs, and building identity.

ISSN: 2582-6433

But there's a downside. The explosion of cyber space has led to a spike in online crimes targeting women. Unlike traditional crimes, online offences are marked by:

1. Hidden, anonymous abusers
2. Damage that can quickly spread out of control
3. Digital content that never really disappears
4. Jurisdiction issues that cross borders

Women often land in the crosshairs—facing more sexualized abuse, threats, and exploitation in these digital spaces. NCRB reports show that cybercrime complaints by women are on the rise, which reflects both a real increase and the fact that more women are coming forward.

Thankfully, the Constitution offers solid protections:

1. Article 14: Equality before the law
2. Article 19(1)(a): Freedom of expression
3. Article 21: Right to life, liberty, privacy, and dignity

The Supreme Court in Justice K.S. Puttaswamy v. Union of India (2017) also made it clear—privacy includes the right to control your own information. Cyber crimes strike directly at this, putting personal data at risk and undermining autonomy.

In Shreya Singhal v. Union of India (2015), the Court stressed balancing free speech with limits, which shapes how tech companies are held accountable.

This paper looks at cyber crimes against women through a constitutional and socio-legal lens, and asks:

1. What underlying factors drive cyber crimes against women?
2. Why aren't current laws enough to protect victims?
3. What reforms can help make the digital world safer for women?

LITERATURE REVIEW

Over the past ten years, the conversation about cyber crimes against women has changed. Early research treated cybercrime as a tech or security issue, often overlooking the role of gender. Now, more experts see it as a deeply gendered problem—rooted in structural inequality and human rights concerns.

Danielle Keats Citron's work really shifted the dialogue. She argued that online harassment

ISSN: 2582-6433

isn't just an annoyance—it undermines women's civil rights and silences them in public life. Mary Anne Franks zeroed in on non-consensual intimate imagery (NCII), framing it as a violation of bodily autonomy that deserves special legal protection.

Shoshana Zuboff introduced the idea of "surveillance capitalism." Digital platforms turn people's data into economic assets, often at their expense. When it comes to women, their personal data is often weaponized—used for abuse, stalking, or fraud.

Indian scholars have added another layer, pointing to how patriarchy shapes both the crimes themselves and society's response. Women who go through online abuse may face blame, stigma, or just get ignored by institutions. Digital illiteracy and a lack of awareness about legal help also make them even more vulnerable.

But there are still gaps in the research. There's not enough work connecting legal analysis with fast-changing technology—especially with the rise of AI-driven harms like deepfakes. Many legal studies don't use available data, which leads to a gap between theory and what happens on the ground. And the real-world challenges of policing these crimes in India are often overlooked.

This paper steps in to help fill those gaps. I draw on legal analysis, real data, and insights on culture and society to give a complete picture of cyber crimes against women in India.

METHODOLOGY

This study uses a mix of doctrinal and analytical methods, combined with some real-world data and global comparisons, to look at cyber crimes against women in India. The doctrinal part means I go through legal texts, case law, and regulations to spot loopholes or inconsistencies and suggest improvements.

Key primary sources include:

1. The Information Technology Act, 2000
2. The Indian Penal Code, 1860
3. The Digital Personal Data Protection Act, 2023
4. The Constitution (Articles 14, 19, 21)

ISSN: 2582-6433

I analyze significant judgments like Justice K.S. Puttaswamy v. Union of India (2017) and Shreya Singhal v. Union of India (2015) to understand privacy, dignity, and free speech in the digital world.

Secondary sources cover NCRB crime stats, UN Women reports, academic journals, and policy briefs—these help ground the analysis and reveal trends.

The research unfolds in four key steps:

1. Identifying and classifying different types of cyber crimes against women
2. Mapping out which laws apply
3. Assessing how well these laws and systems work, using both legal reasoning and data
4. Proposing reforms, drawing from global best practices

I also look to international experiences, mainly from the EU and the US, to shape recommendations that make sense for India but also reflect what's working elsewhere.

TYPOLOGY OF CYBER CRIMES AGAINST WOMEN

Cyber crimes against women keep shifting and growing as technology and online habits change. There's no single face to these crimes—they come in all shapes but connect in disturbing ways.

Let's start with cyberstalking. This isn't just someone lurking online. It's ongoing harassment or intimidation through digital channels, and it often gives offenders a mask of anonymity. They keep at it, feeding off the fear and insecurity they create. Women are frequent targets, and the threat never really feels far away.

Online harassment and trolling are everywhere. These include threats, hate-filled messages, and misogynistic comments. Women with a public profile—journalists, activists, politicians—face the brunt. Most of the time, the goal is clear: push women out of the public conversation and into silence. Then there's the ugly world of non-consensual intimate imagery—better known as revenge porn. Someone shares private photos or videos without permission. This isn't just a privacy violation; it wrecks dignity and can carry deep, lasting scars.

Deepfake technology is a newer twist. AI creates fake but convincing images or videos, usually sexualized and aimed at women. Deepfakes crank up the threat and make digital exploitation

ISSN: 2582-6433

even easier.

Identity theft and impersonation are also rampant. Offenders use stolen personal information to make fake profiles or commit fraud, leaving a wake of emotional, reputational, and sometimes financial damage.

Financial cyber fraud is another threat. Think phishing, blackmail, or scam transactions. Because of digital divides and fewer resources, women—especially those with limited digital literacy—are common targets.

Often, these crimes overlap. Victims might find themselves facing several attacks at once. That's why we need legal and policy responses that go beyond just checking boxes.

LEGAL FRAMEWORK

When it comes to India's laws on cyber crimes against women, the picture is patchy and often a step behind. There isn't a single, unified law that's built for the digital age, especially when it comes to gendered crimes.

The main law is the Information Technology Act, 2000. It talks about privacy and obscene content (Sections 66E, 67, 67A), but only in a basic sense. New threats like deepfakes and AI-created content barely get a mention.

The Indian Penal Code tries to fill the gaps—Section 354D tackles cyberstalking, while Sections 499 and 509 address defamation and insult to modesty. But these provisions date back to a time when "cyber" wasn't even a word in most people's vocabulary. They don't fit the digital world.

In 2023, the Digital Personal Data Protection Act stepped in with a focus on data safety and consent. It's a step forward, but it skips over cyber harassment altogether and pays little attention to how data actually gets abused.

Courts have played a part. In Puttaswamy, the Supreme Court recognized privacy as a fundamental right. Shreya Singhal was about platform liability. Still, big questions about digital crime remain unresolved.

ISSN: 2582-6433

Right now, India's legal tools feel scattered, reactive, and not nearly strong enough for the messy reality women face online.

ENFORCEMENT FAILURES

Having a law on paper is one thing. Making it work? That's where things break down. Many women don't even report cybercrime. Fear of not being believed, social stigma, and little faith in police all feed into this silence. Data shows most cybercrimes never get reported.

And if someone does file a complaint, things often stall right there. Police struggle to register FIRs quickly and don't move fast enough to collect digital evidence before it disappears.

A big issue is that law enforcement just isn't trained for cyber cases. Many officers lack basic digital forensics skills, especially outside big cities.

It doesn't help that so many cybercrimes are cross-border or involve multiple states. Coordination is tough, evidence is murky, and attackers hide easily.

So, conviction rates are low. Digital evidence is tricky, and criminals know how to cover their tracks. All this makes it tough to actually hold anyone accountable. In the end, offenders walk free more often than not.

SOCIO-CULTURAL DIMENSIONS

You can't separate cybercrime from the bigger picture—how society views women. These aren't just tech problems; they're rooted in old biases.

Patriarchal attitudes mean women still get blamed for harassment online—whether for what they post, what they wear, or who they interact with. Victim blaming makes women keep quiet, afraid of how their own families or communities might react.

The digital divide widens the risk. Rural women and those with less education have fewer tools to protect themselves and often don't know where to turn if they're targeted.

The psychological fallout is often devastating—anxiety, depression, isolation. Some stories take a tragic turn, linking persistent harassment to self-harm or worse.

ISSN: 2582-6433

On top of that, families often urge women to just "step back" from the digital world. That restricts education, work, and social interaction—reinforcing old limits in a supposedly new world.

Ultimately, cybercrime against women reflects the same gender inequality that shows up everywhere else.

SOCIAL AWARENESS

Tackling cybercrime isn't just about law and tech—it's about changing minds.

Schools and colleges need to get serious about digital safety. Kids should learn early how to protect themselves online.

Wider awareness campaigns matter too. People need to know their rights, reporting options, and ways to stay safe. The government, NGOs, and community organizations have to work together to build a culture that values digital responsibility.

Support systems—counseling, helplines, legal aid—are just as crucial. Training law enforcement to be more sensitive can make a big difference.

In the long run, changing hearts and habits means challenging victim-blaming and pushing for true gender equality online.

COMPARATIVE ANALYSIS

Look at how India compares to other countries and you'll see clear differences.
The European Union has strict data laws and takes the lead on prevention, user rights, and platform accountability. The United States is focused on issues like platform liability, free speech, and the latest threats—like deepfakes.

India's mostly still reacting to problems as they appear, with outdated laws and weak enforcement.

The lesson? India needs to build more prevention into regulations, make digital platforms answerable, and put victims at the center of policy.

ISSN: 2582-6433

REFORM FRAMEWORK

A real solution to cybercrime against women has to tackle everything at once.

Legislative Reform

1. Pass laws that go after cyber crimes against women specifically.
2. Ban and punish the creation of harmful digital content.
3. Set tougher penalties so offenders think twice.

Technological Measures

1. Use AI to identify abusive content.
2. Make content verification and watermarking mandatory to discourage fakes.

Institutional Strengthening

a. Set up dedicated cybercrime units.
b. Use fast-track courts to get justice moving.
c. Train law enforcement in digital investigations.

Victim-Centric Approach

a. Allow for anonymous complaints.
b. Offer accessible psychological and legal support.

Social Reform

a. Run strong awareness and sensitization programs nationwide.
b. Break down gender prejudices.

CONCLUSION

India's battle with cybercrime against women is complex, deep-rooted, and growing. Digital spaces open huge doors for women's empowerment, but they also carry new dangers.

The current legal system sets a foundation, but it isn't enough to meet the sheer scale and tangled nature of these crimes. Weak enforcement, societal barriers, and low awareness keep the problem alive.The way forward isn't just more laws or fancier tech. It has to be big—legal reform, real investments in enforcement, tech innovation, and a shift in how society thinks. Only with a plan that brings all this together will India make its digital world safe and fair for women.

ISSN: 2582-6433

BIBLIOGRAPHY

Primary Sources

a. Constitution of India, 1950
b. Information Technology Act, 2000
c. Digital Personal Data Protection Act, 2023
d. Indian Penal Code, 1860

Cases

a. Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1
b. Shreya Singhal v. Union of India (2015) 5 SCC 1

Books

a. Danielle Keats Citron, Hate Crimes in Cyberspace (Harvard University Press, 2014)
b. Shoshana Zuboff, The Age of Surveillance Capitalism (Profile Books, 2019)

Journal Articles

a. Danielle Keats Citron and Mary Anne Franks, 'Criminalizing Revenge Porn' (2014)
b. Robert Chesney and Danielle Citron, 'Deepfakes and the New Threat to Privacy' (2019)

Reports

a. National Crime Records Bureau, Crime in India Reports (2024–2026)
b. UN Women, Technology-Facilitated Gender-Based Violence Reports
c. Reserve Bank of India, Cyber Fraud Reports

Online Sources

a. Ministry of Electronics and Information Technology (MeitY)
b. National Cyber Crime Reporting Portal (India)