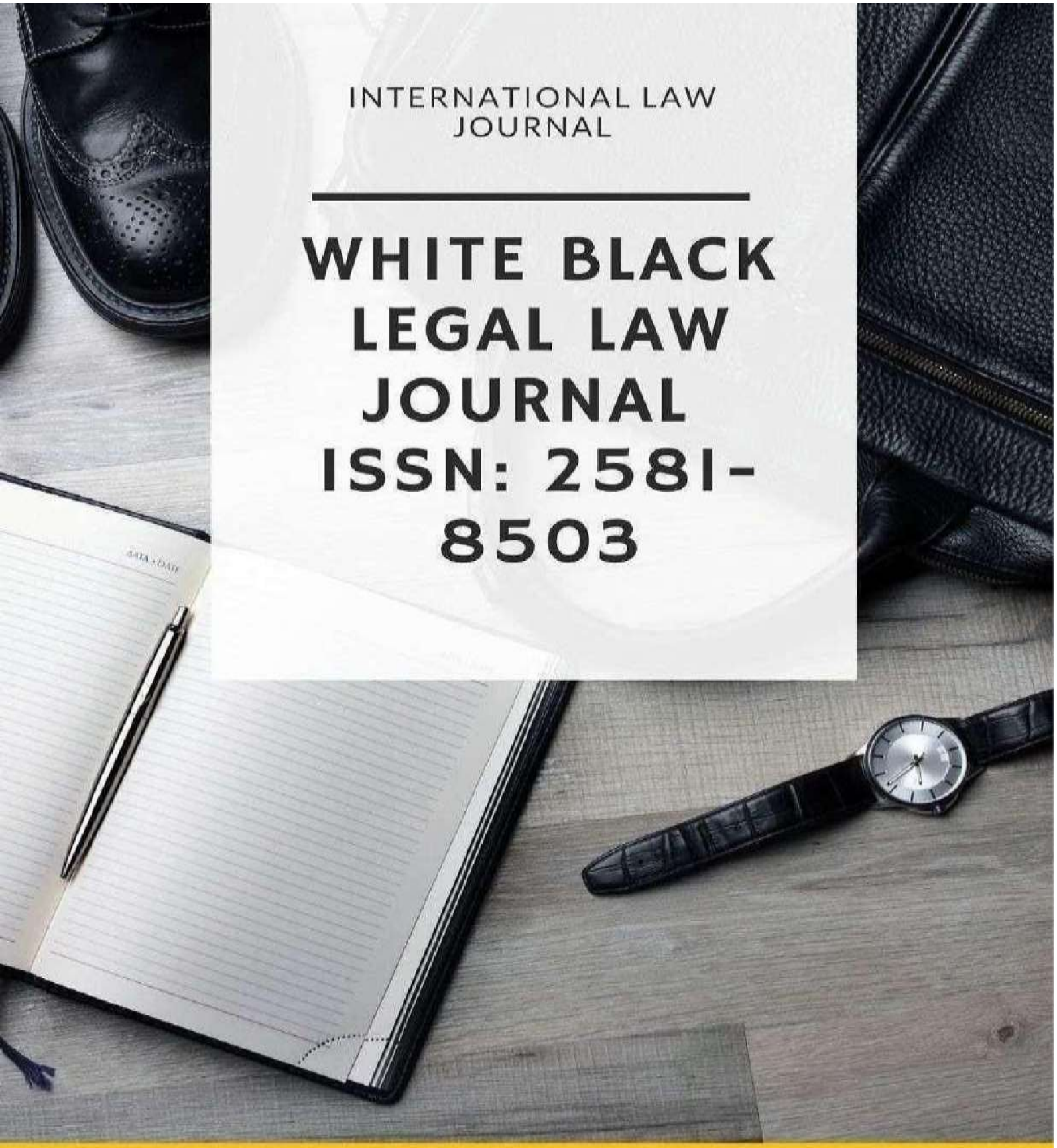

INTERNATIONAL LAW JOURNAL

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.

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.

CYBER THREATS AGAINST WOMEN IN THE DIGITAL AGE: A DOCTRINAL AND FEMINIST LEGAL ANALYSIS

AUTHORED BY - ISHITA RATHORE
Amity Law School, Amity University Noida

Abstract

The fast-changing digital landscape is causing significant disruptions across human interactions, business transactions, government, and social life. At the same time, the changes brought about by the development of digital networks have made the internet an ubiquitous platform for gendered aggression. The current wave of cyber-violence against women is not a random act of online misbehavior. Rather, it constitutes a more efficient and scalable continuation of structural violence against women in the modern age of technological innovation.

This article offers a comprehensive analysis of cyber-aggression from the perspective of both legal theory and feminist research. It identifies five different types of gender-specific violations in the contemporary digital landscape: spatial stalking, algorithmic harassment, image-based abuse, doxxing, and AI deepfakes. This work posits that the technical framework of the online platforms used to perpetrate these offenses actively promotes aggressive activity through anonymity, engagement-oriented structure, data permanency, and transnational reach.

In light of the new forms of digital violence, it is clear that we urgently need a complete reform of the current regulatory regime. This process should focus on the concept of criminality based on consent, platform accountability, and gender-sensitive internet regulation.

1. Introduction: The Digital Public Square as a Contested Terrain

The digital revolution has entirely reshaped the framework within which modern society exists.

Man is not able to see the digital world only as an auxiliary tool anymore. The internet has turned into the social world in which we all live, from the scheduling apps on our phones that organize our day to the platforms on which communities can connect irrespective of hemispheres. The internet is the nervous system of our interactions today. For women, the digital boom that took place brought with it a genuine hope for liberation. Women were able to build their online businesses in ways that could allow them to ignore the barriers created by physicality. Feminist activism became amplified

around the world, and access to learning and opportunities was made available to women living in conservative societies, where movement was strictly regulated.

However, an interesting paradox is present in the digital world. The same system that was built to create equality between people is being used to spy, intimidate, and harm women. Despite being egalitarian when it comes to access, it becomes dangerous territory for individual security.

Gender-based cyber violence cannot be written off as a case of accidental bugs, trolling incidents, or the random behavior of a segment of society that is not being regulated. Online gendered violence is embedded in the architecture of the online public space. The internet is a sophisticated economic system that operates under the logic of data extraction, algorithmic engagement optimization, and patriarchy that has moved from offline spaces to computer coding.

In order to understand this issue, we need to make a critical distinction between cybersecurity and cybersafety. In conventional political rhetoric, these two terms are often used interchangeably, leading to legislation that fails to address the problem.

- Cybersecurity is an infrastructure-related term, it deals with the hardware and software defenses like encryption, firewalls, and system-access controls that work toward preserving the security of the network and preventing any external intrusions into the software. It is mainly concerned with protecting data and infrastructure.
- Cybersafety, by contrast, is solely related to human beings. It means having the ability of a woman to live, express herself, and socialize on the Internet without compromising her privacy, dignity, and security, which may be put at risk by the abusers using cyber space against her.

The current framework focuses more on providing protection to systems than to individuals, and even with a securely protected system, a person may still be vulnerable. In such a situation, a woman can have a digitally protected profile with multi-factor authentication and encryption yet still be highly insecure. If an aggressor has been able to combine all public data about her to ascertain her precise location or create her explicit appearance using generative AI, the digital system is secure but the human entity is helpless.

This paradigm of thinking becomes more pronounced when considering that in the past, open public spaces were considered dangerous zones for women, while private domestic space provided a safe haven from external aggression. The digitized world has eroded this barrier. With the help of portable smartphones, laptops, and other digital equipment, the public domain has been integrated into the privacy of people's homes. The aggressor's harassment of the woman is followed into her private space wherever she goes and at whatever time she finds refuge.

In addition, the characteristics of digital data create an incredibly frightening degree of permanence with regard to victimization. Where, in the physical realm, the abuse is often fleeting and contained by the short-lived memory of those around, the digital space presents a reality where data is permanent and infinitely scalable. A private image, personal data, or a deep-fake video can be uploaded to the internet and instantly replicated, cataloged by search engines, and distributed across decentralized servers worldwide. Rather than dissipating over time, it continues to resurface and creates an unending state of victimization.

Despite the changes in the structural nature of violence, the legal system has yet to adequately address these concerns within the framework of its current laws and regulations that measure digital harm against physical crime, industrial-era evidentiary standards, and property-centric concepts of harm. Our cyber laws were developed to address the issue of white-collar economic crimes, hacking, intellectual property violations, and data breaches. They did not anticipate the use of the internet as a tool for identity-based violence, systematic gender discrimination, or psychological harm.

Through an intensive doctrinal and feminist analysis of the laws of India, this paper explores the critical comparison between the Information Technology Act, 2000 and the newly promulgated Bharatiya Nyaya Sanhita, 2023. This research paper offers insights into how the real-world experiences of cyber-violence along with the architecture of these platforms can lead to the creation of a new legal system based on consent and human dignity.

2. Research Methodology

In this study, there is a qualitative legal research design that will be applied, which is particularly designed for analyzing the tension between advancing technology and stagnant laws. In order to effectively analyze how legislations are dealing with technology-enabled gendered violence, the study will be conducted using two different perspectives simultaneously, blending doctrinal legal analysis and feminist jurisprudence.

The doctrinal analysis portion of this method will conduct an intensive assessment of the primary sources of law. This means that the legislation that will be critically assessed are the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, along with the Supreme Court judgments and judgments from other high courts of various states in India. It will assess how statutes can keep up with current technological advancements.

In tandem with the above analysis based on statutory principles, a critical feminist jurisprudential theory is used here to uncover the underlying dynamics of neutrality that characterize the language of law. By relying on existing theory in relation to the systems of patriarchy, power, and "the

silencing effect," this method of inquiry helps to critically examine the notion of obscenity, modesty, and harm.

Far from taking cyber laws as mere technical provisions, an intersectional analysis of digital networks reveals them as highly political and social entities. This enables the author of the current paper to engage with the broader impact that algorithms, intermediaries, and criminal law may have on gender-based inequality in society, which leads to limiting women's autonomy in the digital world. The primary sources used in this paper include:

- Statutory Instruments: The Information Technology Act, 2000; the Bharatiya Nyaya Sanhita, 2023; the Bharatiya Nagarik Suraksha Sanhita, 2023; and the Digital Personal Data Protection (DPDP) Act, 2023.
- Judicial Precedents: Key rulings from the Supreme Court of India and various state High Courts that address cyberstalking, identity manipulation, non-consensual intimate imagery, and privacy violations.

The secondary sources include academic journal articles that analyze cyber law, criminological research on tech-related abuse, policy documents on international laws and policies related to human rights and internet security (UNHRC, OECD frameworks), and feminist theories on legal discourse.

3. Objectives of the Study

To address the gap between technological advancement and legal protection, this study focuses on five central objectives:

1. To map the evolution of gendered cyber threats within the modern digital landscape,
2. Exploring how traditional forms of violence are transformed by internet architecture.
3. To provide a clear legal taxonomy of digital harms targeting women, including spatial stalking, algorithmic harassment, image-based abuse, doxxing, and generative AI deepfakes.
4. To evaluate the adequacy of the Indian legal response, specifically examining the gaps within the Information Technology Act, 2000, and the newly enacted Bharatiya Nyaya Sanhita, 2023.
5. To analyze the psychological and social costs of digital violence, assessing how online abuse leads to self-censorship and excludes women from the digital public square.
6. To develop a consent-focused, gender-responsive policy manifesto that outlines specific legislative reforms and establishes clear standards for platform accountability.

4. Understanding the Spectrum of Cyber Threats Against Women

4.1 The Continuum of Digital Violence and Platform Architecture

Cyber violence against women cannot be viewed as a set of unrelated, independent acts of online misbehavior. Cyber violence against women is actually a digital evolution of the historically rooted phenomenon of violence against women. From the feminist perspective, violence against women is an evolutionary continuum that moves between the micro-aggression and verbal attacks in public places to domestic manipulation and physical violence in the private spheres of women's lives. The digital technologies did not alter the nature of violence against women; they simply became an integral part of this continuum allowing abusers to utilize new means of enforcing power and fear beyond the boundaries of the state.

The distinctive feature of this age is not the criminal intent itself, but its amplification through the technological characteristics of internet infrastructure. This paper identifies three principal characteristics of cyber violence against women as structural elements enhancing the damage done to women victims.

The permanence of Internet content leads to repeated trauma for victims. Even in the case when a victim receives a court order compelling an offender to remove an offending image from a particular website, it may still continue to exist in backup files, file-sharing systems, and cache memories of search engines.

It follows that the women who occupy these very prominent positions in the public eye, such as journalism, politics, academics, and human rights activism, become targets of systematic oppression. These attacks on women in public do not usually occur in an attempt to instigate ideological discussion; the aim is systematic exclusion. By flooding these women with threats, abusers create an enormous "silencing effect," which forces them either to censor themselves or exit public discourse altogether.

4.2 Cyberstalking and the Surveillance Environment

Where cyberstalking used to be about sending multiple, unsolicited communications to someone's online account, it now entails elaborate monitoring that is ongoing and uninterrupted. The initial reaction of the Indian government to combat the issue took place in relation to the 2001 case of Ritu Kohli. In the said case, the defendant impersonated the identity of the victim by using her account name to log into chat rooms on the internet. She was then subjected to constant harassing phone calls because her private number was disseminated online with overt invitations for contact.

Although the problem of impersonation via digital technology back in 2001 already provided

insights regarding the threats associated with modern spatial surveillance, current surveillance methods are increasingly complicated.

By the year 2026, with the help of GPS systems, continuous check-ins on social media, IoT devices, and commercial networks designed to harvest consumer data, spatial stalking has become a reality. Now, stalking is not about actively communicating with another individual but passively monitoring their whereabouts and activities without the need for any direct interaction.

For instance, stalkers might use Bluetooth tags invisible to the naked eye that will be affixed to the woman's purse or hack into household devices. The metadata derived from social media postings, albeit trivial, is equally useful in this context.

This stalking environment is enabled primarily through commercial data broker firms, which harvest publicly available information, such as registry records, voter registration data, and social media profiles, and assemble a detailed dossier that reveals an individual's personal and private information, including the addresses, employers, families, and habits of those individuals. That information is subsequently sold to anyone via a commercial search engine without verifying their identity and intentions.

Through this process, stalking has been commodified and made significantly more accessible. An individual lacking technical expertise can easily buy an elaborate profile of a targeted individual for surveillance purposes.

The main stalking law we have in India, section 354D of the IPC (which has now been incorporated into the BNS), was crafted against a paradigm of stalking involving constant communication or overt surveillance. The law fails to effectively tackle instances of covert surveillance, in which case the abuser does not seek any communication at all with the woman; he just tracks her location data.

4.3 Online Harassment, Swarming, and Systemic Silencing

In many cases, online harassment occurs through organized, concerted attacks referred to as "swarming." This form of abuse is best exemplified by the landmark case of Kalandi Charan Lenka v. State of Odisha (2017), where a High Court of Orissa faced a situation where a campaign using fake identities, morphed images, and defamatory information was created with the sole purpose of damaging the reputation of a young woman in social circles.

Swarming techniques are organized in nature. A typical swarming exercise starts with the "seed account," such as that of an influencer or even an automated node with followers. A false allegation or attack on the woman is made from this account and amplified by the bot network set up to spread hashtags related to this content. Within hours of the incident, thousands of users get involved in spreading hatred by piling up threats of violence and sexual abuse.

Because of the sheer numbers involved, such assaults are practically unmanageable through conventional means such as blocking or muting on social media platforms. The mental toll of this assault on one's senses is enormous; it causes the constant feeling of being afraid and paranoid. Since the assault is carried out by an anonymous crowd of people all around the world and not a person residing locally, it is impossible for the victim to pinpoint the source of the attack or the exact location at which the assault will be carried out in real life. Such mental pressure leads to a strategic retreat from cyberspace.

4.4 Image-Based Abuse and the "Obscenity Trap"

The non-consensual dissemination of intimate imagery (NCII) constitutes an extreme form of invasion of one's bodily privacy and respectability in cyberspace. This is exemplified in State of Tamil Nadu vs. Suhas Katti, which marked the first-ever criminal case based on cyber law in India. In the case, the defendant had put up derogatory and graphic statements together with the victim's personal contact information on an online chat group where she had previously declined his marriage offer. It was only through Section 67 of the IT Act that the courts managed to convict the offender, setting an important judicial precedent for the legal protection of women's honor online.

However, much has changed in terms of the technological advancement behind such abuses. Back when Suhas Katti committed his offenses in 2004, one would need to have the deliberate intention of posting their material online, especially because of slow internet access and centralized hosting services. Today, the same can be done automatically with an intimate photo spreading from one website to another, including those dealing with adult content, as well as to peer-to-peer message forums.

The primary issue in India is that our legal system is still ensnared within the "obscenity trap." Since there is no specific consent-based statute under Indian law that pertains to image-based sexual abuse, prosecutions must make extensive use of sections 67 and 67A of the Information Technology Act, which punish the publication or distribution of obscene or sexually explicit images.

These clauses were designed within the context of 19th-century Victorian values relating to public morality rather than the human rights of individuals. These laws determine the indecency of an image based on whether it is deemed "explicit" enough to deprave and corrupt the minds of the general public.

As a consequence, the victim becomes a target in their own legal case. For example, proving the explicit nature of the image inevitably involves a detailed examination of the victim by the investigating officers, lawyers, and even judges in the courtroom.

However, this paradigm considers the body of the victim as being a vehicle of social misconduct

rather than that of personal abuse. On the other hand, in contemporary society, as exemplified by the jurisdiction of the United Kingdom, the law on such crimes adopts a paradigm based on consent, whereby the crime entails sharing a sexual image without the consent of the image owner.

4.5 Doxxing: Turning Online Hostility into Physical Danger

Doxxing refers to the malicious release of a person's private details such as their residence address, phone number, direct email address, ID number, and work address. Although doxxing may target anyone, the targeting of women through doxxing presents a particularly gendered offense. Doxxing often comes along with a clear call for sexual assault, transforming online aggression into a real-life danger.

The specific harm caused by doxxing is that doxxing blurs the line between online and offline aggression. Once someone's personal contact information is released online together with malicious statements, she will no longer be safe from her aggressors since they know where she lives, and can physically stalk and confront her, invade her privacy, and physically assault her.

According to law professor Danielle Citron, doxxing is a form of intimidation meant to drive women out of any form of discussion. For a woman, the act of voicing out an opinion could lead to putting herself at risk of being assaulted at home or with her loved ones.

Although the magnitude of this threat cannot be underestimated, there is no express provision for the act of doxxing within India's cyber law, which means that prosecution in such cases would involve the combination of various provisions within the IT Act and the BNS, including Sections 66C (identity theft) of the IT Act and Section 506 (criminal intimidation) of the BNS. This piecemeal approach does not sufficiently address the particular form of damage caused by doxxing, namely, the deliberate and concerted use of public information to mobilize a mob against the victim.

4.6 The Deepfake Crisis: Generative AI and the Weaponization of Likeness

Deepfaking is an important paradigm shift in online abuse of women. Deepfaking involves the use of complex Artificial Intelligence, such as Generative Adversarial Networks (GAN), to fabricate audio, visuals, and videos that are nearly impossible to distinguish from genuine records. The working principle of GAN is basically two algorithms competing against each other – one creates fake pictures while the other checks these pictures against genuine ones and identifies inconsistencies.

During this process, the generator creates ultra-realistic imagery that cannot be distinguished by

humans or conventional detectors. By 2026, the availability of affordable consumer applications using generative AI will have shifted this practice significantly. No technical skills or pricey computers are required for someone to take advantage of GAN technology. An ordinary cell phone and a single photograph of the victim will allow for the creation of an explicit video within minutes. For women, however, the technological transformation strips away the crucial defense of their presence. In the past, a woman had the option of defending herself from defamatory images by proving that she was not there at the time of the photo shoot. But now, with deepfakes, that defense is no longer available since any woman who shares her profile online will have created sufficient visual material to train an AI algorithm.

Moreover, our present legislative definitions of such acts do not cover these circumstances. As per Section 66E of the IT Act which talks about violation of privacy, the offender is required to capture unauthorized images of the private parts of an individual through some electronic means. This does not hold true for images that are fabricated by a machine.

Again, Sections 67 and 67A are also not suitable as they are related to offenses against modesty which is different from an injury to likeness. It is an injury to an individual's digital identity and an infringement of her right to determine her own identity.

5. The Indian Legal Framework: A Doctrinal Critique of Shields, Gaps, and Human Cost

5.1 The Information Technology Act, 2000: A Structural Anachronism

However, the principal legislation regulating cyberspace within India is still the Information Technology Act, 2000. Although the Act itself has gone through various modifications, the basic framework of the statute has not been changed because it dates back to the moment of creation. The IT Act has been established with the purpose of ensuring the security of the economic system by legally supporting electronic commerce, facilitating the process of making transactions, endorsing electronic signatures, and combating cybercrimes against money. The crimes included into the list of punishable actions related to network security, unauthorized access to computer resources, and data theft.

However, the Act was created for the protection of infrastructure, not human rights, which makes it ineffective in the case of combating gender-based cybercrimes. Since the statute views these cases from the technical side, it lacks all the necessary instruments to deal with cyber offenses. However, amendments added to the Act in 2008 have extended the Act to include provisions for violations of privacy (Section 66E) and dissemination of explicit material online (Sections 67A and 67B).

5.2 The Intermediary Liability Loophole: Section 79 and Algorithmic Immunity

One major hurdle to platform accountability in relation to cyber laws in India is that of the safe harbor provision included in Section 79 of the IT Act that gives blanket immunity to network intermediaries such as social media networks, search engines, and other communication platforms against liability for all information or content available through such platforms. This safe harbor provision has been introduced in order to ensure the growth of the Internet without making these platforms liable for any content they have not generated themselves.

This protection of platforms against liability is a consequence of the traditional assumption of the neutrality of technology platforms. However, in the year 2026, social media platforms will no longer be considered mere neutral intermediaries but curators of content using engagement algorithms to promote certain content and generate maximum clicks. As already highlighted earlier, these engagement algorithms are used to disseminate toxic content, including harassment campaigns and doxxing.

The present interpretation of Section 79 creates a major loophole for platforms. According to the law, they must take down any illegal content that they come across only when they receive "actual knowledge" through a court order or a government notification, which was defined in Shreya Singhal vs. Union of India (2015). The law puts undue pressure on the aggrieved party, which is expected to pursue lengthy court procedures to obtain orders against the dissemination of offensive information, while such material continues to be circulated globally.

5.3 The Bharatiya Nyaya Sanhita, 2023: Missed Opportunities for Comprehensive Codification

The adoption of the Bharatiya Nyaya Sanhita (BNS), replacing the IPC of 1860, is considered to be an important step towards modernization of the criminal justice system in India. On closer analysis of this new legislation, one can see how poorly it addressed the need for a coherent set of regulations concerning digital gender-based violence in contemporary times. In fact, the adoption of the BNS failed to produce a more modern approach to tech-facilitated crimes, as it retained the definition of such offenses from the old IPC almost completely.

For instance, the definition of stalking provided by Section 354D of the IPC has been incorporated into the BNS with only slight changes made to its structure. This means that the law continues to define the act of stalking by focusing on physical or electronic means of monitoring, thereby omitting the concept of passive spatial surveillance and digital data brokerage and tracking.

Sections related to criminal intimidation, defamation, and modesty violations also retain their focus on physical aspects of committing crimes. Therefore, when it comes to prosecuting offenders for doxxing, cyber swarming, and deepfakes, authorities are faced with the challenge of adapting these concepts to the existing language of laws.

5.4 The Constitutional Mandate: Puttaswamy and the Right to Digital Safety

The problems of the implementation of statutory laws differ vastly from the progressive approach taken by the Indian judiciary regarding its constitutional interpretation. The Supreme Court of India in the case of Justice K.S. Puttaswamy v. Union of India in 2017 brought revolutionary changes to the legal interpretation of the concept of privacy in the age of information and communications technology. All nine judges agreed that privacy is a constitutional unalienable fundamental right protected by Article 21 of the Constitution.

Specifically, the case of Puttaswamy clarified that privacy consists not only of general personal but also informational privacy and bodily autonomy. Informational privacy means the right of an individual to regulate the flow of personal information over the network, making the practice of unauthorized data aggregation and doxxing illegal. Bodily autonomy goes further and means protection not only of the body but also of the digital representation of an individual's personality against artificial intelligence manipulation.

This constitutional requirement raises cyber security to a level beyond mere regulation but one of human rights. In other words, the government must ensure that the lives and dignities of its people are not violated through cyber-attacks. Nonetheless, such an elaborate constitutional understanding of cyber security is yet to be translated into statutory law, hence leaving a huge disparity between the rights as per the Supreme Court ruling and the actual experience of women at police stations.

6. Judicial Efficacy and Enforcement Challenges

In order to comprehend the impact of these legislative deficiencies on tangible results, it is necessary to explore the practical challenges associated with the Indian judicial system. Despite the high courts' progressive constitutional decisions, the reality of seeking justice at the local grassroots level highlights the presence of significant institutional friction that emerges through three key phases: the initial access point at the local police station, the scientific examination phase at the laboratory, and the trial phase in court.

The first challenge lies in accessing the local police station, where victims of cyberstalking and doxxing attempt to register a First Information Report (FIR). In most cases, such a request is

immediately denied, primarily due to the fact that local police officers often lack adequate education in handling such cases. As a result, officers tend to view non-violent harassment as a personal conflict between two people.

Another institutional hurdle is the forensic logjam. In prosecuting digital crimes, maintaining the electronic chain of custody is essential. According to Section 65B of the Indian Evidence Act (merged with the Bharatiya Sakshya Adhiniyam, 2024), there should be strict certifications along with the electronic documents, which include details about the hash values, device metadata, and extraction reports.

Unfortunately, India's forensic science laboratories in the states suffer from chronic backlogs, resulting in delays that take several years in processing electronic evidence. In situations where deepfakes or automated bot swarms are involved, our state-level forensics departments lack the technology to distinguish between fabricated AI images and the real picture, causing further delays that stop the prosecution process before any court proceedings.

Lastly, at the trial stage, there is a chance of secondary victimization. Since there are no dedicated cyber benches in India's courts, such cases are tried in regular criminal courts, whereby if the crime is prosecuted through the moral obscenity charge, the defense strategy focuses on vilifying the victim's character.

The victims undergo intense cross-examinations about their personal life, their love affairs, and their motives behind taking the photographs. The atmosphere created here is not conducive to the reporting of cases; rather, it becomes an area where victims undergo secondary trauma.

7. A Seven-Point Manifesto for Digital Dignity

In order to align Indian cyber law with the challenges of modern-day online harms, it is imperative that we move away from our paradigm of cybersecurity based on technology to a human rights-based approach centered around consent, dignity, and platform responsibility. The following manifesto lays out a seven-point agenda for such a legal shift:

7.1 Codify a Standalone Cyber Dignity Act Rooted in Consent

The time has come for us to depart from outdated and morally subjective statutes such as Sections 67 and 67A of the IT Act. It is imperative for legislators to create a single, consolidated Cyber Dignity Act that clearly delineates crimes such as image-based sexual abuse, doxxing, spatial stalking, and the making of deepfakes. More importantly, the statute must employ lack of personal consent as the fundamental criteria, instead of moral judgments regarding decency.

This would help the investigation process to be centered around the actions of the perpetrator, not the victim's way of life or personality.

7.2. Abolish Safe Harbor Immunity for Algorithmic Promotion

A sweeping legal immunity that has been conferred on technological platforms through the IT Act needs to be amended. There shall be no safe harbor provisions if the algorithmic mechanisms of the platform promote content that is malicious in nature, such as doxxing data, harassment campaigns, or consensual deep fakes. The platform must be held accountable for the decisions that have been coded into its software structure.

7.3 Establish a Mandatory Two-Hour Rapid Takedown Standard

In cases of highly damaging forms of abuse, such as non-consensual intimate videos and deepfakes, the existing notice and takedown periods are alarmingly long. This manifesto demands an absolute two-hour rule, statutorily mandated. Once the victim files a proper notification regarding any form of non-consensual explicit material, it should be mandatory that the platform takes down the offensive content within a two-hour period globally. In case they fail to meet this deadline, they will face hefty fines and lose their safe harbor status for that particular instance.

7.4 Create Trauma-Informed, Women-Led Forensic Units

In order to ensure that enforcement challenges at the community level are overcome, it is necessary for every police station to have a cyberdesk managed by women. The staff in such cyberdesks must be trained in digital forensics, detecting deepfakes, and analyzing metadata, thereby being able to collect evidence without causing further suffering to the victims.

7.5 Introduce Digital Restitution and Global De-indexing Remedies

Restoring the digital reputation of the victim is the core consideration that our criminal justice system needs to address, and not necessarily punishing the wrongdoer. The criminal justice system ought to have the power to give an order of digital restitution. This order would compel search engines and other internet intermediaries to globally de-index, delist, and delete the offending material from their search caches.

7.6 Reform the DPDP Act to Enforce Contextual Consent

It is necessary to update the provisions of the DPDP Act, 2023, in order to fix the loophole in relation

to the definition of "publicly available data." This means that just because someone uploads some data on a publicly accessible platform for a particular purpose (like maintaining a professional profile), it cannot become grounds for granting third parties the right to scrape such data and use it for something completely different.

7.7 Integrate Digital Ethics and Consent into National School Curricula

Cyber safety on a long-term basis cannot be solely addressed by punishment, but rather needs to evolve into a cultural change in the way people behave online. It will involve teaching digital ethics, privacy hygiene, and bystander culture within national educational curriculums. By educating youth about treating the internet like a social space where they need to respect other individuals' consents and dignity, they will become more responsible online.

Conclusion

The present analysis of cyber violence against women makes it clear that cyber threats for women do not represent a series of random incidents that occurred with the advent of a digital world. These are, instead, a scaled version of violence against women in the past and are enabled through a set of unique features associated with today's internet space that thrive within an attention economy that frequently relies on creating chaos. Existing laws which try to deal with these issues through traditional frameworks that focus on physical violence and morals are inadequate.

Our laws have indeed made considerable progress in recognizing privacy as a constitutional right as evident from the Puttaswamy judgment. However, the daily implementation and protection of this right is flawed and disassociated from the constitutional perspective of cyber laws. Cyber safety for women cannot be attained simply by telling women to stay away from public spaces, close down their social media profiles, and tighten up their security settings.

Creating a democratic digital public sphere requires fundamental legal restructuring. Instead of a technology-centered approach to "cybersecurity," India must adopt a people-centered framework of "cybersafety" that values human dignity and respect as core elements of cyberspace law.

Implementing consensual laws regarding crimes against women in cyberspace, enforcing platform accountability, and ensuring swift implementation will help India create a cyberspace where technology is used as a means to empower women, not marginalize them.

References

Statutes and Legislation

- The Information Technology Act, 2000 (Act No. 21 of 2000), India.
- The Information Technology (Amendment) Act, 2008, India.
- The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023), India.
- The Bharatiya Nagarik Suraksha Sanhita, 2023, India.
- The Bharatiya Sakshya Adhiniyam, 2023, India.
- The Digital Personal Data Protection Act, 2023, India.

Landmark Judicial Decisions (India)

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- State of Tamil Nadu v. Suhas Katti, 2004 (Cyber Crime Case, Trial Court, Chennai).
- Kalandi Charan Lenka v. State of Odisha, 2017 SCC OnLine Ori 125.
- Ritu Kohli Case, 2001 (First reported cyberstalking case in India).
- Subramanian Swamy v. Union of India, (2016) 7 SCC 221.
- Avnish Bajaj v. State (NCT of Delhi), 2005 (Bazee.com case).

Books and Academic Works

- MacKinnon, Catharine A. Toward a Feminist Theory of the State. Harvard University Press, 1989.
- MacKinnon, Catharine A. Are Women Human? Harvard University Press, 2006.
- Citron, Danielle Keats. Hate Crimes in Cyberspace. Harvard University Press, 2014.
- Inness, Julie C. (ed.). Privacy, Intimacy, and Isolation. Oxford University Press, 1992.
- Lyon, David. Surveillance Society: Monitoring Everyday Life. Open University Press, 2001.
- Zuboff, Shoshana. The Age of Surveillance Capitalism. PublicAffairs, 2019.
- Lessig, Lawrence. Code and Other Laws of Cyberspace. Basic Books, 1999.

Journal Articles and Policy Reports

- United Nations Human Rights Council (UNHRC), Reports on Online Violence Against Women and Girls.

- Organisation for Economic Co-operation and Development (OECD), Protecting Women and Girls Online (Policy Report).
- Franks, Mary Anne. "Unwilling Avatars: Idealism and Discrimination in Cyberspace," Columbia Journal of Gender and Law.
- Citron, Danielle Keats. "Cyber Civil Rights," Boston University Law Review.
- OECD. Addressing Online Gender-Based Violence (2022).
- World Health Organization (WHO), Reports on Digital Violence and Mental Health Impacts.

Cyber Law and Technology Reports

- International Telecommunication Union (ITU), Reports on Cybersecurity and Cybercrime.
- National Crime Records Bureau (NCRB), Crime in India Reports (latest editions).
- CERT-In, Government of India, Cybersecurity Guidelines and Advisories.
- NASSCOM, Cybersecurity and Digital India Ecosystem Reports.

Comparative and International Legal Frameworks

- Australia, Online Safety Act 2021 (as amended).
- Office of the eSafety Commissioner (Australia), Safety by Design Framework
- United Kingdom, Online Safety Act 2023.
- European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679.

WHITE BLACK LEGAL