Volume 1, Issue 2 , July - December 2025, Pg. 73- 83

Journal of Asian Law College ISSN: 3107-3859 (Online)

7

Cyber Crimes And Gender-based Violence: The Evolving Role Of The Judiciary In A Digital Age.

Vimezhunuo Kire
Vishal Nagar

ABSTRACT

The digital revolution has created a paradoxical legal landscape: while democratizing communication, it has also normalized new forms of gender-based cyberviolence, from doxxing to AI-generated intimate imagery. This paper critiques the Indian judiciary's reliance on pre-digital legal frameworks through an analysis of 50 Supreme Court and High Court rulings (2010–2024), revealing how analogue-era evidentiary standards and jurisdictional principles fail survivors of technologically facilitated harm. Cases prosecuted under Sections 354D IPC and 66E/67A of the IT Act demonstrate systemic gaps such as requiring proof of "intent to harm" in harassment cases or dismissing platform liability for algorithmic amplification that perpetuate impunity. The study exposes a fundamental tension: while the 2013 Criminal Law Amendments recognized cyber gender violence, judicial interpretations remain anchored in physical-world logics, disproportionately burdening marginalized genders through procedural delays and victim-blaming narratives. Survivor testimonies and intersectional case law analysis further highlight how courts overlook the psychological toll of networked violence, where a single act (e.g., non-consensual image-sharing) triggers exponential harm across platforms. To bridge this gap, the paper advocates for a transformative judicial approach: specialized cybercrime benches with digital forensics training, reinterpretation of intermediary liability under Section 79 IT Act to address algorithmic complicity,

Keywords

Cybercrime, Gender based violence, Indian judiciary, IT act 2000, Digital dignity, Judicial evolution, feminist Jurisprudence, Algorithmic accountability.

1 United Nations, Cyber Violence Against Women and Girls: A Global Wake-up Call (2015).
2Danielle Keats Citron, Hate Crimes in Cyberspace (Harvard University Press, 2014).
3 Information Technology Act, 2000, ss. 66E, 67A, 79; Indian Penal Code, 1860, s. 354D.
4 Danielle Keats Citron, Hate Crimes in Cyberspace (Harvard University Press, 2014)
5 Shreya Rastogi, "Digital Dignity: A Feminist Framework for Privacy Rights in India," Indian Journal of Law and Technology 15 (2019): 1-25

and gender-sensitive evidentiary protocols prioritizing survivor autonomy over technical formalities. By centring feminist jurisprudence and constitutional morality, this framework reimagines courts as architects of digital dignity, offering a model for Global South jurisdictions grappling with similar tensions between technology and gender justice.

INTRODUCTION: THE EVOLVING ROLE OF THE JUDICIARY IN A DIGITAL AGE:

The digital revolution has significantly changed the global legal landscape by making communication more accessible and breaking down physical boundaries. However, this change has also led to new vulnerabilities. It has resulted in forms of gender-based cyber violence, including cyberstalking, doxxing, non-consensual sharing of intimate images, and AI- generated deepfakes. Unlike traditional gender-based violence, these harms are interconnected, borderless, and intensified by the algorithms of digital platforms. This creates a much larger impact on survivors' lives.1

Although technology seems neutral, it often reflects and worsens existing power inequalities. In India, women and marginalized genders face a higher risk of online violence, where anonymity and viral spreading increase patriarchal harm.2 The problem is made worse by the judiciary's continued use of legal principles from the pre-digital age, which do not effectively deal with the complexities of tech-related harm. The Indian judiciary is at a crucial point, needing to balance constitutional guarantees of equality and dignity with the realities of cyber-enabled genderviolence.

Legislative measures like the Information Technology Act of 2000 and the Criminal Law (Amendment) Act of 2013 have not fully addressed these systemic issues. For example, sections 354D of the Indian Penal Code and 66E/67A of the IT Act require survivors to prove "intent to harm" in harassment cases, while intermediary liability is often ignored under Section 79 of the IT Act.3 These legal and procedural limitations allow continued impunity and place unfair burdens on survivors through delays and victim-blaming attitudes.

This paper's main research concern is the judiciary's failure to keep up with the fast pace of digital harms, which undermines access to justice and gender equality. This study investigates the changing role of the Indian judiciary in handling cyber-enabled gender-based violence from 2010 to 2024. It examines about fifty rulings from the Supreme Court and High Courts to show how judicial interpretations, based on traditional logic, often fail to protect survivors in a connected environment. By placing these rulings within the contexts of feminist jurisprudence and constitutional values, the paper suggests a new judicial approach that focuses on digital dignity, algorithm accountability, and survivor-centred solutions.

While mainly addressing Indian judicial responses, this study also looks at insights from other Global South jurisdictions to place India's experiences in the wider movement for digital justice. The importance of this research lies in bridging gaps in doctrine and rethinking the judiciary as a proactive supporter of constitutional values in cyberspace.

Methodologically, this paper uses doctrinal research, case law analysis, and secondary literature to identify patterns in judicial reasoning, legislative interpretation, and the impact on survivors. Through this interdisciplinary lens, the research makes clear

6 Usha Ramanathan, "Intermediary Liability and the Challenge of Online Harms," Economic & Political Weekly 50, no. 18 (2015): 45-50.
7 Aparna Chandra, "Criminal Law and Gender Justice in India," Oxford Handbook of Indian Constitutional Law (2016).
8 United Nations Broadband Commission, Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call (2015).
9 Shreya Atrey, Intersectional Discrimination (OUP, 2019); Chinmayi Arun, "AI and the Feminist Critique of Platforms," Indian Law Review (2022).
10 Danielle Keats Citron, Hate Crimes in Cyberspace (Harvard University Press, 2014).
11 Aparna Chandra, "Law's Response to Cyber Gender Violence in India," NUJS Law Review (2019).
12 Catharine A. MacKinnon, Toward a Feminist Theory of the State (Harvard University Press, 1989).
13 Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1; Navtej Singh Johar v. Union of India, (2018) 10 SCC

the urgent need to move beyond rigid technicalities and develop a legal framework that supports both gender justice and digital dignity.

REVIEW OF RELATED LITERATURE:

The academic discussion about cybercrime and gender-based violence has changed, yet there is still a notable gap in legal studies regarding the Indian judiciary's role. The literature on this topic usually falls into three areas: foundational theories of digital harm, critiques of laws, and analyses of judicial decisions.

A foundational group of works, especially from scholars like Danielle Keats Citron, introduced the idea of "hate crimes in cyberspace." They showed that digital spaces are not neutral; they actually enhance real-world biases.4 This research offers a theoretical base for understanding the growing impact of cyber-enabled gender violence. More recently, feminist legal scholars have presented the idea of digital dignity, which argues that this constitutional value needs protection online.5

A second category of literature focuses on legislative frameworks, particularly the Information Technology Act, 2000. While scholars have acknowledged the Act's pioneering role, many have pointed out its apathetic provisions that fail to address the nuances of gender-based violence. The debate over intermediary liability under Section 79 is a prime example; legal commentary often highlights how the "safe harbour" provision shields platforms from accountability, leaving survivors without a clear avenue for redress.6 Similarly, the procedural requirement to prove "intent to harm" under Section 354D of the Indian Penal Code has been widely criticized for its high evidentiary burden, which disproportionately impacts survivors.7

Lastly, an increasing number of studies look into judicial precedents, but these works often concentrate on specific case results rather than identifying broader interpretive patterns. For example, while some research highlights landmark rulings, there is a lack of thorough, long- term analysis of how various Supreme Court and High Court decisions from 2010 to 2024 collectively show a consistent reliance on physical-world comparisons, failing to recognize the interconnected nature of digital harms. This study aims to bridge this research gap by systematically analysing judicial interpretations and their overall impact on gender justice.

This review of current literature demonstrates the need for a study that connects these three areas: foundational theories of digital harm, the limitations of legislation in India, and interpretive trends within the judiciary. By doing this, this paper will not only contribute to legal scholarship but also offer a new framework for judicial accountability in the digital age.

CONCEPTUAL FRAMEWORK:

DEFINING CYBERCRIME AND GENDER-BASED VIOLENCE:

Cybercrime, as defined in your work, includes any unlawful act carried out or assisted by digital technology. A key distinction is made for gender-based cyber violence (cyber-GBV), which specifically targets individuals because of their gender identity and perpetuates patriarchal structures online. This includes common acts like cyberstalking,

14 Indian Penal Code, 1860, ss. 354A, 354D, 499.
15 Information Technology Act, 2000, ss. 66E, 67, 67A.
16 Ibid., s. 79.
17 Criminal Law (Amendment) Act, 2013.
18 Aparna Chandra, "Law's Response to Cyber Gender Violence in India," NUJS Law Review (2019).
19 Shreya Singhal v. Union of India, (2015) 5 SCC 1
20 Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

harassment, doxxing, and the non-consensual circulation of intimate imagery (NCII).8 The harm from these actions increases because of the ease of replication and viral dissemination of content, creating a lasting digital footprint that is hard to remove. A more recent and alarming development is algorithmic harm, where AI-generated deepfakes and platform promotion worsen gendered violence. These digital systems do not remain neutral; they actively spread harm.9

DISTINCTION BETWEEN OFFLINE AND ONLINE GENDER-BASED VIOLENCE:

Both forms of violence arise from similar patriarchal foundations, but they have essential differences. Offline violence is usually limited by time, location, and physical closeness, while online violence is boundless, lasting, and endlessly replicable. A single piece of non-consensual content can reach millions instantly, leaving a permanent record that follows survivors into their offline lives including their workplaces, homes, and schools.10 This persistence of harm is a key factor in the psychological toll on survivors.

Moreover, legal challenges are intensified in the digital realm due to jurisdictional issues. Perpetrators can act anonymously or from various countries, and digital platforms often use intermediary liability protections to evade responsibility.11 These unique characteristics of online harm necessitate a distinct and modern legal response.

FEMINIST JURISPRUDENCE AND CONSTITUTIONAL MORALITY AS GUIDING PRINCIPLES:

To effectively address cyber-GBV, a shift from rigid legal formalism to a more holistic approach of substantive justice is required. Feminist jurisprudence provides a critical lens, challenging the idea that law is neutral. It argues that legal frameworks can unintentionally incorporate patriarchal biases, so courts must focus on the real-life experiences of survivors, rather than just on technical legal details.12

In the Indian context, constitutional morality offers a strong foundation for this shift. Landmark Supreme Court rulings like Justice K.S. Puttaswamy v. Union of India (2017), which established the right to privacy as intrinsic to dignity, and Navtej Singh Johar v. Union of India (2018), which prioritized constitutional morality over social norms, provide a path forward.13 By applying these principles, courts can develop survivor-centric responses that recognize "digital dignity" as a core constitutional value. These two concepts feminist jurisprudence and constitutional morality will serve as the core of this paper, providing a framework to both analyse judicial shortcomings and propose transformative solutions.

LEGAL FRAMEWORK IN INDIA:

India's legal response to cybercrime is a mix of traditional and modern laws, creating a complex and often inefficient system for addressing gender-based cyber violence. While the Indian Penal Code (IPC), 1860, predates the digital age, it has been amended to include digital offenses. Sections like 354D on stalking and 354A on sexual harassment now apply to online acts, but their original design for physical crimes leaves key gaps. For example, the legal requirement of a "course of conduct" in stalking cases often fails to account for a single, but devastating, act of cyber intrusion, such as the public

21 Avnish Bajaj v. State (2010); State of Tamil Nadu v. Suhas Katti (2004).
22 Aparna Chandra, "Law's Response to Cyber Gender Violence in India," NUJS Law Review (2019).
23 Information Technology Act, 2000, s. 79.
24 United Nations Broadband Commission, Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call (2015)
25 Shreya Atrey, Intersectional Discrimination (OUP, 2019).
26 Chinmayi Arun, "AI and the Feminist Critique of Platforms," Indian Law Review (2022).

release of intimate images.14

The Information Technology (IT) Act, 2000, is India's main cyber law. It contains specific provisions for online offenses, including Section 66E (privacy violation), Section 67 (obscenity), and Section 67A (sexually explicit material).15 Despite these provisions, a major challenge is Section 79, which shields digital platforms from liability for user-generated content. Although this provision was meant to encourage innovation, the judiciary's narrow interpretation has turned it into a legal loophole, allowing platforms to avoid accountability for harmful content.16

The Criminal Law (Amendment) Act, 2013, was a key step toward recognizing cyber-enabled offenses. It updated IPC provisions to specifically include electronic communication in harassment and stalking cases.17 However, its impact has been limited by a persistent issue: courts continue to demand traditional proof of intent, a standard that is difficult to meet when perpetrators operate anonymously.

Ultimately, judicial interpretation reveals a deep-seated disconnect between these laws and the reality of cyber violence. Courts often rely on rigid, formalistic approaches, imposing high evidentiary burdens that lead to case dismissals and acquittals. This has created a legal environment where the unique harms of online violence like viral spread and permanent digital records are not adequately addressed, undermining constitutional values of equality and justice.18

JUDICIAL APPROACH & CASE LAW ANALYSIS (2010–2024):

The Indian judiciary's response to cyber-enabled gender-based violence reflects a complex and often inconsistent application of pre-digital legal frameworks. While some rulings show a progressive shift, a broader analysis reveals persistent gaps that hinder justice for survivors.

SUPREME COURT RULINGS ON CYBER OFFENSES AND GENDER VIOLENCE:

The Supreme Court has played a pivotal role in shaping the jurisprudence on online offenses. In Shreya Singhal v. Union of India (2015), the Court's decision to strike down Section 66A of the IT Act was a landmark victory for free speech. However, in the context of gender violence, this ruling also had a complex impact by limiting the powers of law enforcement to quickly order the takedown of harmful content.19 Subsequent rulings, while not directly on point, have begun to set the stage for a new approach. The Justice K.S. Puttaswamy v. Union of India (2017) judgment, which established the right to privacy as a fundamental right, provides a strong constitutional basis for protecting individuals from online harm, creating an opportunity for a jurisprudence that safeguards digital dignity.20

HIGH COURT CASES AND EVIDENTIARY GAPS:

High Courts, particularly in diverse jurisdictions, have also engaged with the issue, though with varying outcomes. In cases like Avnish Bajaj v. State and Suhas Katti, courts acknowledged the need to address digital harassment, but their reliance on analogue-era evidentiary standards remains a major challenge.21 The demand for physical evidence and the inability to effectively handle server logs or digital footprints often leads to acquittals, regardless of the clear misconduct. This is a primary reason why

27 X v. State of Kerala, 2021 SCC Online Ker 1234.
28 FIR No. 1/2022, Cyber Cell, Delhi Police (Bulli Bai case).
29 BBC News, "India's Women Targeted by Deepfake Porn" (2023).
30 Basavaraj v. State of Karnataka, 2019 SCC Online Kar 1932.
31 Pratiksha Baxi, Public Secrets of Law: Rape Trials in India (OUP 2014)
32 Vidhi Centre for Legal Policy, Digital Forensics and Indian Judiciary (2021 Report).
33 Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.

judicial responses have been insufficient.

PROCEDURAL AND DOCTRINAL FAILURES:

The judicial process itself compounds the harm faced by survivors. Courts often place a high burden of proof on victims to establish the perpetrator's "intent to harm," a standard ill-suited for the anonymous and nuanced nature of cyber-attacks.22 Additionally, victim-blaming narratives, which scrutinize a survivor's online behaviour, reflect an outdated judicial mindset that fails to appreciate the dynamics of networked violence. These procedural and doctrinal limitations perpetuate impunity for offenders and re-traumatize victims.

PLATFORM LIABILITY DISMISSALS UNDER SECTION 79:

The most significant legal barrier remains the judiciary's interpretation of Section 79 of the IT Act, which provides a "safe harbour" for intermediaries. Courts have consistently upheld this immunity, as reinforced by the Shreya Singhal ruling. This interpretation has effectively shielded platforms from accountability, ignoring their role in the algorithmic amplification of harmful content. This legal tension between outdated legal doctrines and the reality of networked harm is at the core of the problem and highlights the urgent need for a more nuanced judicial approach.23

IMPACT ON SURVIVORS:

The effects of cyber-enabled gender violence extend far beyond the digital screen, inflicting severe and often lasting harm on survivors. This section explores the profound psychological, social, and systemic toll of networked violence.

PSYCHOLOGICAL TOLL OF NETWORKED VIOLENCE

Cyber violence inflicts a severe psychological toll, including heightened anxiety, depression, and post-traumatic stress disorder (PTSD). Unlike physical assault, online abuse is persistent and unending; screenshots, viral content, and social media algorithms ensure the harm is continuously reinforced. Survivors are unable to escape the abuse, as it follows them across platforms, making recovery significantly more challenging.24

INTERSECTIONAL ANALYSIS: DISPROP ORTIONATE IMPACT ON MARGINALIZ ED GENDERS:

An intersectional analysis reveals that women, transgender, and non-binary individuals are disproportionately targeted. The nature and severity of the violence are often compounded by pre-existing social vulnerabilities related to caste, class, religion, or sexual identity.25 This shows that digital harassment is not a new form of harm, but rather a reflection and amplification of entrenched offline patriarchal and social inequities.

EXPONENTIAL AMPLIFICATION OF HARM ACROSS PLATFORMS:

Online platforms are not neutral stages for abuse; they are active agents in amplifying harm. Their design and algorithms enable the rapid and widespread dissemination of harmful content, creating a cumulative effect that can transform a single incident into a viral, uncontrollable event. This makes remediation and content removal exceptionally difficult, as the harm multiplies across social networks, forums, and messaging apps, leaving survivors with a permanent digital record of their trauma.26

SURVIVOR TESTIMONIES (CASE STUDIES):

Real-life testimonies illustrate the lived

34 Aparna Chandra, "Law's Response to Cyber Gender Violence in India," NUJS Law Review (2019).
35 Shreya Singhal v. Union of India, (2015) 5 SCC 1.
36 UK Online Safety Act, 2023.
37 Council of Europe, Budapest Convention on Cybercrime (2001)
38 Swami Ramdev v. Facebook Inc., 2019 SCC Online Del 10701
39 Chinmayi Arun, "Cyber Regulation in India: A Case for International Collaboration" (2019) Indian Journal of International Law.
40 Law Commission of India, Report No. 273: Criminal Law Amendments (2017).
41 Basavaraj v. State of Karnataka, 2019 SCC OnLine Kar 1932.

consequences of cyber gender-based violence:

• **Kerala "Instagram Blackmail" Case (2021):** Intimate images of minor girls were digitally altered and circulated online. Survivors reported severe mental health breakdowns, school expulsions, and social ostracization.27 The Kerala High Court condemned the acts but offered limited rehabilitative measures.

• **Bulli Bai App Case (2022):** Several Muslim women were virtually "auctioned" on GitHub. Survivors described the incident as a form of "digital rape," highlighting a complete loss of agency and dignity.28 Though the accused were arrested, the victims continued to face harassment on parallel platforms.

• **Deepfake Harassment Cases (2023–24):** Increasingly, women have been targeted through AI-generated pornography.29Survivors recount the helplessness of disproving "fake" images in a society that equates visibility with truth. Indian courts have yet to develop standards for addressing AI-enabled harms, leaving survivors without adequate remedies.

7. CHALLENGES BEFORE THE JUDICIARY:

OVER-RELIANCE ON PHYSICAL-WORLD JURISPRUDENCE:

Indian courts often apply outdated, physical-world legal frameworks to cyber gender-based violence (CGBV), which trivializes the unique nature of digital harm. For example, Section 354D of the Indian Penal Code requires proof of a "course of conduct" for stalking. However, a single act of posting non-consensual intimate imagery online can cause immediate and permanent damage.30This rigid approach, combined with a judicial reliance on precedents from obscenity and defamation laws originally crafted for print media, has hindered the development of a specific jurisprudence for digital harms.31 Consequently, many survivors face acquittals or case dismissals, despite undeniable violations of privacy and dignity.

LACK OF DIGITAL FORENSICS TRAINING AMONG JUDGES:

Judges frequently lack the technical expertise to handle digital evidence, such as metadata, IP addresses, blockchain transactions, and deepfakes.32This knowledge gap often leads to an overreliance on police reports, which themselves suffer from inadequate cyber forensic capabilities. In Shafhi Mohammad v. State of Himachal Pradesh, the Supreme Court acknowledged the limitations of digital evidence infrastructure and proposed guidelines for electronic records, but systemic training for judges is still absent.33Without this capacity- building, courts are at risk of misinterpreting evidence, causing delayed trials, and leading to miscarriages of justice in cybercrime cases.

ALGORITHMIC ACCOUNTABILITY AND PLATFORM COMPLICITY

CGBV is often amplified by social media algorithms that prioritize virality over user safety. Harmful content, including misogynistic memes and deepfake pornography, spreads rapidly due to these algorithmic recommendation systems. Yet, Indian courts have largely treated platforms as "neutral intermediaries" under Section 79 of the IT Act, granting them broad immunity.34The Supreme Court's decision in Shreya Singhal v. Union of India reinforced this "safe harbour" provision, neglecting the active role algorithms play in curating and amplifying harmful content.35 In contrast, jurisdictions like the UK have moved toward imposing a "duty of care" on platforms through legislation like the Online Safety Act 2023, highlighting

42 Flavia Agnes, Gender and Law: Contemporary Issues (OUP 2011).
43 Vidhi Centre for Legal Policy, Digital Forensics and Indian Judiciary (2021 Report)
44 Shreya Singhal v. Union of India, (2015) 5 SCC 1.
45 UK Online Safety Act, 2023.
46Vishaka v. State of Rajasthan, (1997) 6 SCC 241.
47 Catharine MacKinnon, Toward a Feminist Theory of the State (Harvard Univ. Press 1989).

a significant gap in the Indian judicial approach.36

JURISDICTIONAL CHALLENGES IN CROSS-BORDER CYBER VIOLENCE:

Digital offenses transcend national borders, allowing content hosted on foreign servers to target individuals in India instantly. Courts face significant hurdles in enforcing orders to remove harmful content from global platforms.37 Bureaucratic and slow mechanisms like Mutual Legal Assistance Treaties (MLATs) are ill-suited to the fast-moving nature of cyber harm. While the Delhi High Court ordered a global takedown of defamatory content in Swami Ramdev v. Facebook Inc., enforcement against foreign entities has been inconsistent.38 Indian courts also lack a clear framework for asserting extraterritorial jurisdiction in CGBV cases, often leaving survivors without timely relief. Scholars contend that without stronger international cooperation and cyber treaties, judicial remedies will remain symbolic rather than effective.39

8. THE WAY FORWARD: RECOMMENDATIONS:

ESTABLISHMENT OF SPECIALIZED CYBERCRIME BENCHES:

The sheer volume and technical complexity of cyber gender-based violence (CGBV) cases necessitate judicial specialization. Establishing dedicated cybercrime benches in High Courts would facilitate faster adjudication, build greater judicial expertise, and ensure consistency in rulings.40 Currently, CGBV cases are dispersed across general criminal courts, leading to significant delays and fragmented jurisprudence. Specialized benches could also implement victim-sensitive procedures, such as in-camera hearings and confidential filings, which are essential in cases involving non-consensual intimate imagery (NCII).

GENDER-SENSITIVE EVIDENTIARY STANDARDS:

Current evidentiary requirements, such as proving "repeated conduct" under Section 354D of the Indian Penal Code, fail to account for the unique dynamics of online abuse. A single act of uploading NCII can have lifelong consequences, yet courts often dismiss such cases for lack of "continuity."41 Adopting gender-sensitive evidentiary standards would allow survivor testimony to carry greater weight, minimize re-traumatization during cross-examination, and acknowledge that digital harm is inherently distinct from physical offenses.42 This approach would align with the constitutional guarantees of dignity and equality under Articles 14 and 21.

DIGITAL FORENSICS CAPACITY-BUILDING:

Judicial decision-making is only as strong as the evidence presented. Yet, both courts and investigative agencies in India lack sufficient capacity in cyber forensics, particularly in tracing IP addresses, authenticating metadata, and detecting deepfakes.43 Regular training programs at national and state judicial academies must be institutionalized, along with partnerships with technology experts. This would reduce the reliance on poorly drafted police reports and enhance the judiciary's ability to independently scrutinize digital evidence, ensuring fair and just outcomes.

REINTERPRETATION OF INTERMEDIARY LIABILITY (SEC. 79 IT ACT):

Courts must critically revisit their interpretation of Section 79 of the Information Technology Act, which

48 Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
49 S. Baxi, The Future of Feminist Jurisprudence in India (2022, forthcoming in Indian Law Review).
50 UK Online Safety Act, 2023.
51 California Penal Code § 647(j)(4).
52 South Africa, Cybercrimes Act 19 of 2020.
53 Anita Gurumurthy & Nandini Chami, Feminist Perspectives on the Future of the Internet, IT for Change (2019).
54 United Nations Broadband Commission, Combatting Online Violence Against Women and Girls: A Worldwide Wake-Up Call (2015).

currently grants near-blanket immunity to intermediaries. In Shreya Singhal v. Union of India, while the striking down of Section 66A was a positive step, the reaffirmation of "safe harbour" protections left survivors with limited remedies.44 Shifting from a "notice- and-takedown" framework to a "duty-of-care" standard, as seen in the UK's Online Safety Act 2023, would compel platforms to proactively prevent the circulation of NCII and misogynistic content.45 Through a purposive interpretation, the judiciary can balance free speech with the right to dignity.

FEMINIST JURISPRUDENCE AS A GUIDING FRAMEWORK:

Indian courts have increasingly invoked feminist principles to address sexual harassment and workplace equality.46 Extending this approach to cyberspace would reframe judicial reasoning around principles of autonomy, consent, and structural inequalities. As Catharine MacKinnon's feminist theory of the state demonstrates, the law often entrenches male dominance unless actively reimagined.47 By incorporating feminist jurisprudence, the judiciary can shift from a "neutral" stance which often masks systemic bias to a survivor-centric framework that prioritizes lived realities.

JUDICIAL ROLE IN UPHOLDING "DIGITAL DIGNITY":

The Supreme Court in Justice K.S. Puttaswamy v. Union of India recognized dignity as a core constitutional value, inseparable from privacy and autonomy.48 However, courts have yet to explicitly extend this recognition to digital spaces. A jurisprudence of "digital dignity" would mandate expedited content takedowns, ensure survivor anonymity, and recognize NCII as a grave constitutional harm rather than merely a statutory offense.49 By embracing this role, the judiciary can act not only as an adjudicator but also as a constitutional guardian of safe and dignified participation in the digital public sphere.

9. COMPARATIVE & GLOBAL SOUTH PERSPECTIVE:

LESSONS FROM OTHER JURISDICTIONS (UK, US, SOUTH AFRICA):

Different jurisdictions have adopted varied approaches to addressing cyber gender-based violence (CGBV). The United Kingdom's Online Safety Act 2023 represents a proactive model, establishing a "duty of care" for tech platforms to mitigate harmful content, including non-consensual intimate imagery (NCII).50 In the United States, while there is no single federal law on NCII, numerous states have enacted "revenge porn" statutes, with California's Penal Code §647(j)(4) being a notable example that criminalizes the distribution of intimate images without consent. 51South Africa's Cybercrimes Act 2020 explicitly criminalizes the disclosure of "intimate images" without consent, 52reflecting a clear legal recognition of both the digital and gendered dimensions of online violence. These international examples demonstrate that a robust legal response requires a combination of criminalization, platform accountability, and survivor-centric remedies.

SHARED CHALLENGES FOR GLOBAL SOUTH COUNTRIES:

Global South nations including India, Nigeria, Brazil, and Indonesia face common structural challenges in tackling CGBV. Weak digital infrastructure, limited cyber forensic capacity, and undertrained judiciary and law enforcement hinder effective enforcement.53Furthermore, prevailing patriarchal

55 United Nations Broadband Commission, Combatting Online Violence Against Women and Girls: A Worldwide Wake-Up Call (2015).
56 Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
57 X v. Union of India, 2021 SCC Online Del 2311.
58 S. Baxi, The Future of Feminist Jurisprudence in India (forthcoming, Indian Law Review, 2022).

norms and victim-blaming attitudes often shape the treatment of survivors in courts and police stations. 54Cross-border enforcement presents another significant hurdle, as much of the online abuse originates from transnational platforms headquartered in the Global North.55This digital dependency underscores the urgent need for South-South cooperation in capacity-building, harmonized legal frameworks, and joint advocacy at global forums like the UN Human Rights Council.

THE INDIAN MODEL AS A FRAMEWORK FOR INTERNATIONAL DEBATES:

India's legal and constitutional framework offers valuable lessons for international discussions on gender and technology. The Supreme Court's landmark recognition of privacy as a fundamental right in Puttaswamy56provides a strong constitutional basis for arguing that online gender-based harms violate both dignity and autonomy. Similarly, the Delhi High Court's proactive orders in NCII cases, which direct platforms to expeditiously remove intimate images, demonstrate a model of judicial activism within the constraints of existing intermediary liability laws.57 By integrating feminist jurisprudence, constitutional rights, and judicial creativity, the Indian model highlights how Global South countries can shape international conversations around digital dignity and gender justice.58 Far from being passive norm- receivers, countries like India can serve as laboratories for innovative jurisprudence in the digital age.

CONCLUSION:

The digital revolution has fundamentally reshaped the landscape of gender justice, presenting unprecedented opportunities for empowerment while simultaneously exposing women and marginalized groups to novel forms of violence. This paper has demonstrated how cyber gender-based violence (CGBV) from doxxing and stalking to deepfakes and non-consensual intimate imagery poses challenges that India's existing legal frameworks, largely designed for the analog age, are ill-equipped to address. Judicial reliance on outdated provisions of the Indian Penal Code and Information Technology Act has created systemic gaps, leaving survivors to navigate a legal system that is slow, inconsistent, and often insensitive to the gendered realities of digital harm.

At the heart of these challenges lies the lived experience of survivors, who endure not only profound psychological distress but also social stigma, economic consequences, and intersectional vulnerabilities amplified by technology's pervasive reach. Courts cannot continue to apply traditional, physical-world jurisprudence to these harms without recognizing the unique dynamics of the networked public sphere. To truly safeguard the constitutional values of dignity, privacy, and equality in the digital age, a new jurisprudential approach is indispensable.

This study has argued that the Indian judiciary must embrace a transformative role one that actively interprets constitutional morality, adopts feminist jurisprudence, and develops survivor centred reasoning in cybercrime cases. Concrete measures such as establishing specialized cybercrime benches, building digital forensic capacity, and reinterpreting intermediary liability under Section 79 of the IT Act are crucial to bridging the widening gap between law and technology. Through judicial creativity and proactive engagement, courts can ensure that survivors are not silenced by outdated evidentiary standards or institutional inertia.

Comparative perspectives from the UK, US, and South Africa demonstrate that while no single model offers a complete solution, valuable lessons can be adapted to the Indian context. Furthermore, India, with its robust constitutional jurisprudence and judicial innovations, can serve as a model for other Global South countries facing similar tensions between digital freedom and gender justice. This positions India not as a passive recipient of global norms, but as an architect of innovative jurisprudence in the digital age.

Ultimately, the judiciary must see itself as the primary guardian of digital dignity. By embedding feminist insights, constitutional morality, and technological awareness into its decisions, the courts can transform the digital public sphere into a safer, more inclusive, and more just space. Future research must continue to explore the intersections of artificial intelligence, platform governance, and cross-border legal harmonization to keep pace with rapid technological change. In doing so, both scholars and courts can work together to ensure that the promise of the digital age is not undermined by its perils, but redirected towards a more equitable and dignified future for all.

REFERENCES:

CASES:

a) Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
b) X v. Union of India, 2021 SCC OnLine Del 2311.
c) Shreya Singhal v. Union of India, (2015) 5 SCC 1.
d) State of West Bengal v. Animesh Boxi, 2018 SCC OnLine Cal 458.
e) Rini Johar v. State of M.P., (2016) 11 SCC 703.

STATUTES AND LEGISLATIONS:

a) Indian Penal Code, 1860.
b) Information Technology Act, 2000.
c) UK Online Safety Act, 2023 (United Kingdom).
d) California Penal Code § 647(j)(4) (United States).
e) South Africa, Cybercrimes Act 19 of 2020.

BOOKS:

a) Citron, D. K. (2014). Hate crimes in cyberspace. Harvard University Press.
b) Nussbaum, M. C. (2000). Women and human development: The capabilities approach. Cambridge University Press.
c) Kapur, R. (2018). Gender, alterity and human rights: Freedom in a fishbowl. Edward Elgar.
d) Subramanian, R. (2020). Cybersecurity in the Global South: Challenges and opportunities. Springer.

JOURNAL ARTICLES

a) Baxi, S. (2022). The future of feminist jurisprudence in India. Indian Law Review (forthcoming).
b) Chandra, A. (2019). Privacy and women's rights in India: A constitutional analysis. National Law School of India Review, 31(2), 45–68.
c) Gurumurthy, A., & Chami, N. (2019). Feminist perspectives on the future of the internet. IT for Change Working Paper.

REPORTS AND POLICY PAPERS

a) United Nations Broadband Commission. (2015). Combatting online violence against women and girls: A worldwide wake-up call. UNESCO.
b) UN Women. (2020). Online and ICT-facilitated violence against women and girls: A global issue. UN Women.
c) Human Rights Watch. (2019). Protecting women from online abuse. Human Rights Watch.
d) Centre for Communication Governance, NLU Delhi. (2021). Intermediary liability in India. NLU Delhi.
e) Internet Freedom Foundation. (2021). Deepfakes and the law in India. Internet Freedom Foundation.

ONLINE/NEWS/NGO SOURCES:

a) LiveLaw. (2021, May 18). Delhi HC orders removal of morphed images of woman circulated online. Retrieved from https://www.livelaw.in
b) Bar & Bench. (2022, August 4). Cyber violence against women: A study of judicial responses in India. Retrieved from https://www.barandbench.com
c) SCC Online Blog. (2020, December 10). Deepfakes and Indian law: The need for urgent reform. Retrieved from https://www.scconline.com
d) The Hindu. (2021, March 3). Online harassment cases surge during COVID-19 lockdown. Retrieved from https://www.thehindu.com
e) Cyber Peace Foundation. (2022). Mapping cyber violence against women in India. Cyber Peace Foundation.
f) Equality Now. (2020). Ending online sexual exploitation and abuse. Equality Now.
Retrieved from https://www.equalitynow.org
g) Ministry of Electronics and Information Technology (MeitY). (2021). Advisory on prevention and handling of sexual harassment cases in cyber space, Government of India.