International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Gender, Technology and Crime

Ms. Rishika Biswas

Student, Law

Abstract

Online harassment represents one of the most urgent socio-legal challenges of the digital age, disproportionately affecting women and gender minorities. In India, the intersection of entrenched patriarchal norms, rapid internet expansion, and an evolving legislative framework creates a complex and often inadequate response to gendered cybercrime. This research paper examines the legal architecture governing online harassment in India, with a particular focus on gender-based dimensions. Drawing on statutory provisions, judicial precedents, governmental data, and feminist legal theory, the paper critically evaluates the Information Technology Act 2000 (amended 2008), the Indian Penal Code, and related legislation. It explores the structural gaps in enforcement, the role of digital platforms in perpetuating harm, and the psychosocial impact of online harassment on victims. The paper further analyzes comparative legal frameworks from the United Kingdom, Australia, and the United States to extract lessons for India. Finally, the paper proposes a set of comprehensive reforms—legislative, institutional, and technological—aimed at building a safer, more equitable digital environment for women and gender minorities in India.

Keywords: Online harassment, cybercrime, gender-based violence, Information Technology Act, India, feminist legal theory, digital safety

1. Introduction

The digital revolution has transformed nearly every aspect of contemporary life in India. With over 900 million internet subscribers as of 2025, India is one of the world's largest and fastest-growing digital economies. Yet this expansion has not been uniformly liberating. For millions of women and gender minorities, the internet has become a site of violence, intimidation, and exclusion. Online harassment—ranging from cyberstalking and non-consensual intimate image sharing to doxxing and coordinated abuse campaigns—has emerged as a critical obstacle to women's full and equal participation in digital public life.

Online harassment is not merely a technological problem; it is fundamentally a gendered phenomenon, rooted in offline patterns of patriarchy, misogyny, and structural inequality. Research consistently demonstrates that women, particularly those who are public, vocal, or from marginalized communities, face significantly higher rates of online abuse than their male counterparts. For women in India, who already navigate deeply entrenched social hierarchies, the digital sphere replicates and amplifies these inequities.

Despite growing public awareness and legislative activity, India's legal framework for addressing gendered online harassment remains fragmented, inconsistently enforced, and in many respects inadequate. The Information Technology Act, 2000 (as amended in 2008), the Indian Penal Code, 1860 (IPC), and the Protection of Women from Domestic Violence Act, 2005, among other statutes, collectively

form an imperfect mosaic of provisions that address some dimensions of the problem while leaving critical gaps. Law enforcement agencies frequently lack the technical expertise, gender sensitivity, and institutional will to respond effectively to cybercrime complaints by women.

This paper undertakes a systematic examination of the legal, social, and institutional dimensions of online harassment in India through a gendered lens. Section 2 reviews scholarly literature and theoretical frameworks. Section 3 maps the scope and typology of gendered online harassment in the Indian context. Section 4 conducts a detailed analysis of the existing legal framework. Section 5 examines the enforcement landscape, including systemic failures. Section 6 compares India's approach with international models. Section 7 assesses the psychosocial impact on victims. Section 8 proposes a comprehensive reform agenda. Section 9 concludes.

2. Literature Review and Theoretical Framework

2.1 Feminist Legal Theory and Cyberspace

The study of gendered online harassment requires an interdisciplinary framework that brings together feminist legal theory, criminology, and digital media studies. Catharine MacKinnon's foundational argument that law is not gender-neutral—but rather reflects and perpetuates male dominance—offers a critical lens through which to evaluate cybercrime statutes. When law is drafted without accounting for women's experiences, it systematically fails to protect them.

Martha Fineman's vulnerability theory provides another valuable framework. Fineman argues that vulnerability is a universal human condition, but that social institutions differentially protect individuals from harm based on race, gender, class, and other axes of identity. Applied to cyberspace, this framework reveals how digital platforms and legal systems can either mitigate or compound women's vulnerability to online abuse.

Patricia Cain and other feminist scholars have emphasized the importance of intersectionality—a concept developed by Kimberlé Crenshaw—in understanding how multiple dimensions of identity shape experiences of discrimination and violence. In India, caste, religion, class, and sexual orientation intersect with gender to produce highly differentiated experiences of online harassment. Dalit women, Muslim women, and LGBTQ+ individuals face compounded forms of abuse that mainstream legal frameworks often fail to address.

2.2 Indian Scholarship on Cybercrime and Gender

Indian scholarship on gendered cybercrime has grown substantially over the past decade. Scholars like Amita Dhanda and Upendra Baxi have examined the limitations of India's colonial-era legal architecture in addressing contemporary digital harms. More recently, researchers at the Centre for Internet and Society (CIS) and the Internet Freedom Foundation (IFF) have produced empirical work documenting the prevalence and impact of online harassment in India, as well as the barriers victims face in seeking legal redress.

The 2020 report by the National Commission for Women (NCW) highlighted a sharp rise in cybercrime complaints by women, particularly during the COVID-19 pandemic when digital dependence increased dramatically. Studies by Roxana Ghiassi and others have explored how algorithmic amplification on social media platforms disproportionately exposes women to abusive content, raising important questions about platform accountability.

2.3 Global Perspectives

International scholarship provides important comparative insights. Work by Danielle Keats Citron in the

United States has been particularly influential, arguing that cyber harassment constitutes a civil rights violation that undermines women's equal citizenship. Citron's advocacy for robust legal responses has informed legislative developments in multiple jurisdictions. Eleanor Jamieson's research in the United Kingdom context has documented the limitations of existing harassment law and the need for platform-level interventions. These international perspectives inform the comparative analysis undertaken in Section 6 of this paper.

3. The Landscape of Gendered Online Harassment in India

3.1 Defining Online Harassment

Online harassment encompasses a broad spectrum of harmful conduct facilitated by digital technologies. For the purposes of this paper, the term refers to any pattern of digital communication, behavior, or content that is intended to intimidate, distress, humiliate, threaten, or harm an individual on the basis of gender or sexual identity. This definition includes, but is not limited to: cyberstalking, online sexual harassment, non-consensual intimate image sharing (commonly termed 'revenge porn'), doxxing (the malicious publication of private identifying information), identity theft and impersonation, and coordinated pile-on or mob harassment.

It is important to distinguish between isolated offensive comments—which, while harmful, may not meet the threshold of harassment—and sustained, targeted campaigns of abuse. The latter are qualitatively more damaging, as they involve deliberate, often coordinated efforts to silence, shame, or harm their targets. In many cases, online harassment transitions into offline threats or physical violence, underscoring its status as a serious safety concern.

3.2 Statistical Overview

The National Crime Records Bureau (NCRB) data reveals alarming trends in cybercrime in India. In 2023, the NCRB registered over 65,893 cybercrime cases across India, representing a compound annual growth rate of approximately 24% over the preceding five years. Women constituted a significant proportion of victims in cases involving cyberstalking, online defamation, and morphing of images. The state of Uttar Pradesh consistently reports the highest absolute numbers of cybercrime cases, though metropolitan cities such as Delhi, Mumbai, Bengaluru, and Hyderabad record high per-capita rates.

However, official statistics almost certainly represent a substantial undercount. Multiple surveys, including the 2022 Digital Equality Survey conducted by the Internet and Mobile Association of India (IAMAI), suggest that the majority of online harassment incidents are never reported to law enforcement. Victims cite fear of social stigma, distrust of police, lack of awareness of legal remedies, anticipated re-traumatization in the legal process, and fear of retaliation as primary reasons for non-reporting.

3.3 Typologies Prevalent in the Indian Context

Several forms of online harassment are particularly prevalent in the Indian context. Cyberstalking, involving the persistent and unwanted monitoring and contacting of a target through digital means, frequently accompanies domestic violence and intimate partner abuse. The expansion of surveillance technologies and social media has dramatically lowered the barriers to stalking behavior. Non-consensual sharing of intimate images—often weaponized against women after relationship breakdowns or as tools of coercion—represents one of the fastest-growing categories of gendered cybercrime.

Coordinated harassment campaigns, often organized through messaging applications like WhatsApp and Telegram, as well as platform-specific mechanisms on Twitter and Instagram, have been used to silence women journalists, activists, academics, and politicians. Notable cases include the Bulli Bai and Sulli

Deals incidents of 2021-2022, in which Muslim women were auctioned on GitHub-hosted platforms in a deeply disturbing act of communal and gendered violence. These incidents exposed critical gaps in both platform governance and legal enforcement.

4. The Legal Framework: Analysis and Critique

4.1 The Information Technology Act, 2000 (Amended 2008)

The Information Technology Act, 2000 (IT Act) constitutes the primary legislation governing cyberspace in India. As amended in 2008, it contains several provisions relevant to online harassment. Section 66A, which criminalized the sending of 'offensive' or 'menacing' messages, was a commonly invoked provision in harassment cases. However, the Supreme Court of India struck it down in Shreya Singhal v. Union of India (2015), holding that it was constitutionally overbroad and violated the freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution.

The removal of Section 66A created a significant gap. While the judgment was rightly celebrated as a victory for free expression, the absence of a carefully drafted replacement has left many victims of online harassment without an effective legal remedy. The court in Shreya Singhal drew a critical distinction between 'discussion' and 'advocacy' on one hand, and 'incitement' on the other—but failed to adequately account for the chilling effect that targeted harassment has on victims' own free expression.

Section 66C (identity theft) and Section 66D (cheating by personation) offer some protection against impersonation-based harassment. Section 66E criminalizes the intentional violation of privacy by capturing, publishing, or transmitting images of a person's private parts without consent, carrying a maximum penalty of three years' imprisonment and/or a fine of two lakh rupees. This provision, while important, is limited in scope and does not comprehensively address non-consensual intimate image sharing in all its forms.

Section 67 criminalizes the publication or transmission of obscene material in electronic form, while Section 67A specifically addresses material containing sexually explicit conduct. Section 67B targets child sexual abuse material. These provisions can apply to certain forms of online sexual harassment, but they are framed in terms of public morality rather than victim-centered harm, and their broad language has sometimes been misused against consensual adult content.

4.2 Indian Penal Code Provisions

Several provisions of the Indian Penal Code, 1860, have been applied to online harassment cases. Section 354A criminalizes sexual harassment, including the making of sexually colored remarks. Section 354C addresses voyeurism, and Section 354D creates the specific offence of stalking, which includes electronic stalking through methods such as monitoring email usage, internet use, and other forms of electronic communication. These provisions were introduced through the Criminal Law Amendment Act, 2013—commonly known as the Nirbhaya Act—in response to the horrific gang rape in Delhi in December 2012 and the nationwide protests that followed.

Section 499 and 500 of the IPC, which govern criminal defamation, can theoretically be applied to online defamation campaigns against women, though their application is complicated by questions of intent and the constitutional protection afforded to free expression. Section 507, dealing with criminal intimidation by anonymous communication, is directly applicable to anonymous online threats.

Section 509, which penalizes any word, gesture, or act intended to insult the modesty of a woman, represents an older provision that has been applied in digital contexts. However, its framing in terms of

'modesty'—a paternalistic and morality-laden concept—has been criticized by feminist legal scholars as reflecting the very patriarchal assumptions that enable harassment.

4.3 Other Relevant Legislation

The Protection of Women from Domestic Violence Act, 2005, while primarily designed to address offline intimate partner violence, has been extended by courts to cover digital forms of abuse within domestic relationships. The Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013 (POSH Act) applies to online sexual harassment within workplace contexts, including harassment through digital communications. The Indecent Representation of Women (Prohibition) Act, 1986, though largely outdated, has occasionally been invoked in cases involving digital content.

4.4 Critical Gaps in the Legal Framework

Notwithstanding these provisions, the legal framework exhibits several critical deficiencies. First, there is no single, comprehensive anti-stalking or anti-harassment statute that consolidates available remedies and provides a clear definitional framework. The fragmentation of relevant provisions across multiple statutes makes navigation of the legal system burdensome for victims, many of whom lack access to specialized legal advice.

Second, the current framework does not adequately address the phenomenon of coordinated mob harassment, in which no single harasser's conduct may individually meet the threshold for criminal liability, yet the collective effect is devastating for the victim. Third, platform accountability remains underdeveloped. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose some obligations on social media intermediaries, but critics argue that they prioritize government oversight over user safety, and that penalties for non-compliance are insufficiently deterrent. Fourth, the framework fails to adequately address the specific vulnerabilities of LGBTQ+ individuals, who face compounded discrimination and are not adequately protected under gender-neutral provisions. The decriminalization of consensual same-sex relations through the Navtej Singh Johar judgment (2018) was a landmark step, but substantive equality in the digital sphere remains elusive for sexual and gender minorities.

5. Enforcement Landscape and Institutional Failures

5.1 Police Response and Gender Sensitivity

Even where the legal framework provides an adequate basis for action, enforcement failures significantly undermine its effectiveness. Women who report online harassment to law enforcement frequently encounter disbelief, victim-blaming attitudes, and a lack of technical understanding among officers. Studies document instances in which police officers have counseled women to delete their social media accounts, reconcile with abusive partners, or abandon complaints on the grounds that the conduct was insufficiently serious. Such responses reflect and perpetuate the broader culture of impunity that enables online harassment.

India's police forces are predominantly male, and women police officers—while increasing in number—remain underrepresented, particularly in senior positions. The absence of mandatory, comprehensive gender-sensitivity training for all police personnel is a critical gap. Specialized cybercrime units exist in major cities, but their capacity is stretched thin, and they often prioritize financial cybercrimes over harassment cases.

5.2 Judicial Response

The judiciary has produced a mixed record in online harassment cases. While some High Courts and the

Supreme Court have handed down important judgments expanding protections for women in digital spaces, lower courts frequently exhibit delays, evidentiary challenges, and gender-insensitive attitudes. The evidentiary requirements for establishing cybercrime can be particularly onerous: preserving digital evidence, establishing identity in anonymous harassment cases, and navigating platform data requests require technical expertise that many complainants—and indeed many legal professionals—lack.

However, there are also notable positive developments. The Delhi High Court has in several cases directed expedited action by cyber police and issued injunctions restraining the further circulation of non-consensual intimate images. In Kalandi Charan Lenka v. State of Odisha (2017), the Orissa High Court upheld the conviction of an accused under Section 66E and Section 67 of the IT Act, affirming that digital privacy violations are serious offences warranting custodial sentences.

5.3 Role of Digital Platforms

Social media platforms and digital intermediaries play an indispensable but frequently inadequate role in addressing online harassment. As the primary venues through which harassment occurs, platforms have both the technical capability and the moral responsibility to implement effective content moderation, reporting mechanisms, and victim support systems. In practice, platforms' content moderation decisions are frequently inconsistent, biased, and slow. Automated systems have been found to disproportionately remove content by marginalized users while leaving harassing content intact.

The IT Rules 2021 mandate that significant social media intermediaries designate nodal officers and grievance officers, and establish a three-tier grievance redressal mechanism. While these requirements represent an improvement over the earlier, more passive intermediary liability regime, their implementation has been uneven and their effectiveness in protecting victims of harassment remains questionable.

6. Comparative Legal Framework

6.1 United Kingdom

The United Kingdom has undertaken significant legislative reform in the area of online harassment. The Online Safety Act 2023 places comprehensive duties of care on social media platforms and search services, requiring them to take proactive steps to protect users from illegal content and, in the case of larger platforms, from legal but harmful content. The Act introduces new criminal offences including the harmful communications offence and the cyberflashing offence. The Malicious Communications Act 1988 and the Communications Act 2003 have also been applied in online harassment cases.

A distinctive feature of the UK approach is the emphasis on platform-level obligations, with the regulator Ofcom empowered to impose substantial fines for non-compliance. This represents a systemic rather than purely reactive approach to online safety—one that places responsibility on powerful intermediaries rather than placing the burden entirely on individual victims to pursue legal remedies.

6.2 Australia

Australia's Online Safety Act 2021 created the position of an Online Safety Commissioner with broad powers to investigate complaints, issue removal notices to platforms, and publish information about platform compliance. The Act covers a wide range of online abuse, including cyberbullying material, non-consensual sharing of intimate images, and cyber abuse of adults. The emphasis on a dedicated regulatory body with enforcement powers offers a potentially instructive model for India.

6.3 United States

The United States presents a more fragmented picture. Section 230 of the Communications Decency Act,

1996, which broadly immunizes platforms from liability for user-generated content, has been credited with enabling the growth of the internet but criticized for removing incentives for platforms to address harassment. State-level laws on cyberstalking, revenge porn, and online harassment vary considerably. Federal legislation such as the Interstate Stalking Punishment and Prevention Act can apply in some circumstances, but there is no comprehensive federal anti-harassment law.

6.4 Lessons for India

The comparative analysis yields several lessons for India. First, dedicated regulatory bodies with enforcement powers and technical expertise appear more effective than relying solely on traditional police and courts. Second, placing proactive obligations on platforms—rather than treating them as passive intermediaries—is essential given the volume and speed of digital communications. Third, a victim-centered approach, including special provisions for expedited relief, anonymity protections, and specialized support services, significantly improves access to justice. Fourth, effective implementation requires sustained investment in training, technology, and institutional capacity.

7. Psychosocial Impact on Victims

The harms inflicted by online harassment extend far beyond the digital sphere. Research consistently documents severe psychosocial consequences for victims, including anxiety, depression, post-traumatic stress disorder (PTSD), social withdrawal, and disruption of professional and personal life. A 2023 study published in the Journal of Cyberpsychology, Behavior, and Social Networking found that women who experienced sustained online harassment reported significantly elevated levels of psychological distress compared to a control group, with effects persisting well beyond the cessation of the harassment itself.

In the Indian context, the social dimensions of online harassment are particularly acute. For many women, online harassment carries the threat of reputational damage in communities where a woman's 'honor' is treated as a collective family asset. The viral spread of intimate images or false allegations can have devastating consequences for marriage prospects, family relationships, and social standing. This social context means that many women face enormous pressure to remain silent about their experiences, which compounds the harm and entrenches the culture of impunity.

Online harassment also exerts a powerful chilling effect on women's participation in public life. Journalists, activists, academics, and politicians report self-censoring their work, withdrawing from social media, and limiting their public engagement as a direct result of online abuse. This silencing effect represents a profound threat to democratic discourse and to gender equality in public life. The self-imposed withdrawal of women's voices from digital public spheres represents a form of secondary victimization that law and policy must urgently address.

For LGBTQ+ individuals, who are disproportionately targeted for online harassment in India, the psychosocial impact intersects with experiences of stigma, family rejection, and social marginalization. The threat of 'outing' as a tool of harassment can be existentially threatening in a social context where same-sex relationships, despite being decriminalized, remain stigmatized in many communities.

8. Toward a Comprehensive Reform Agenda

8.1 Legislative Reform

India urgently needs a comprehensive, standalone Online Safety and Anti-Harassment Act that consolidates existing provisions, fills critical gaps, and adopts a victim-centered framework. Such legislation should clearly define the various forms of online harassment, establish graduated offences and

proportionate penalties, and provide for expedited civil remedies including interim injunctions and takedown orders. The Act should explicitly address coordinated mob harassment, recognize the particular vulnerabilities of LGBTQ+ individuals, and incorporate intersectional considerations of caste, religion, and disability.

The non-consensual sharing of intimate images deserves specific legislative attention, with criminal penalties commensurate with the severity of the harm caused. The UK's approach of creating a specific cyberflashing offence—criminalizing the sending of unsolicited sexual images—also merits consideration. Provisions should be made for the rapid removal of harmful content by platforms, with clear timelines and consequences for non-compliance.

Importantly, any new anti-harassment legislation must be carefully drafted to avoid repeating the mistakes of Section 66A, which was struck down for being overbroad. The legislative framework must be content-neutral where possible, focused on conduct and harm rather than vague notions of 'offensiveness' or 'obscenity,' and firmly grounded in constitutional guarantees of free expression.

8.2 Institutional Reform

India should establish a dedicated National Online Safety Authority (NOSA), modeled on the Australian eSafety Commissioner, with a mandate to receive and investigate complaints, issue binding orders to platforms, conduct public education campaigns, and monitor the effectiveness of online safety measures. The Authority should be adequately resourced, technically sophisticated, and structurally independent of both government and industry. It should include specialist units addressing gendered and identity-based harassment.

Within law enforcement, mandatory, periodic gender-sensitivity and digital literacy training for all police personnel is essential. Specialized cybercrime units should be strengthened with adequate staffing, equipment, and investigative powers. A cadre of specially trained women cyber officers should be developed to ensure that victims have access to sympathetic and knowledgeable responders. Fast-track courts for cybercrime cases, particularly those involving gendered harassment, should be expanded.

8.3 Platform Accountability

Social media platforms and other digital intermediaries operating in India must be held to robust safety standards. The regulatory framework should require platforms above a certain size to conduct and publish regular transparency reports on harassment-related complaints, maintain effective and accessible reporting mechanisms, respond to valid complaints within defined timeframes, and cooperate fully with law enforcement within the bounds of privacy protections.

India should explore the introduction of meaningful platform liability for failure to act on harassment that the platform has been formally notified of, as a targeted exception to the existing intermediary liability framework. Algorithmic amplification of harmful content deserves specific regulatory attention, including requirements for risk assessments and mitigation measures.

8.4 Support Services and Access to Justice

Effective legal remedies are meaningless if victims cannot access them. India must invest significantly in victim support infrastructure. This includes free legal aid for cybercrime victims, accessible digital forensics support for evidence preservation, psychosocial counseling services, and financial assistance where victims have suffered economic harm. National helplines and online reporting portals should be consolidated, well-publicized, and adequately staffed.

Civil society organizations that provide frontline support to victims of online harassment should receive sustained government support. Universities and schools should be required to provide digital safety and

awareness education, including age-appropriate content on online harassment, consent, and bystander intervention.

8.5 Research and Data

Policymaking on online harassment is hampered by inadequate data. The NCRB should develop a more granular and comprehensive taxonomy of cybercrime that disaggregates data by the type of harassment, the gender, caste, religion, and sexual orientation of victims, and the platform or medium involved. Independent academic and civil society research should be supported through public funding. Longitudinal studies tracking the efficacy of legal interventions would provide an invaluable evidence base for policy refinement.

9. Conclusion

Online harassment in India is a multidimensional problem with deep roots in patriarchal social structures, amplified by the affordances of digital technology, and inadequately addressed by existing legal frameworks. This paper has demonstrated that while India has developed a range of legislative provisions relevant to gendered online harassment, these provisions are fragmented, inconsistently enforced, and insufficient to provide effective protection or justice for the majority of victims.

The gendered character of online harassment is not incidental but structural: it reflects and reinforces offline inequalities, silences women's voices in public life, and perpetuates cultures of impunity. Law reform, while necessary, is not sufficient on its own. Effective response requires a comprehensive ecosystem of legislative, institutional, technological, and social interventions, developed through meaningful consultation with affected communities, particularly women, LGBTQ+ individuals, Dalit communities, and religious minorities.

The comparative analysis reveals that other jurisdictions have made meaningful progress through dedicated regulatory bodies, proactive platform obligations, and victim-centered frameworks. India, with its unique constitutional commitments to equality and dignity, has both the obligation and the opportunity to develop a world-class response to gendered online harassment. The stakes are high: nothing less than the conditions of equal citizenship in the digital age are at issue.

As India continues its rapid digital expansion, the question of who can safely participate in online life is a question of democracy itself. A legal and institutional framework adequate to the challenge of gendered online harassment is not a luxury but a prerequisite for a just and inclusive digital society. This paper has sought to contribute to the scholarly and policy debate that must precede and accompany such a transformation.

References

1. Citron, D. K. (2014). *Hate Crimes in Cyberspace.* Harvard University Press.
2. Crenshaw, K. (1991). Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review,* 43(6), 1241-1299.
3. Centre for Internet and Society. (2022). *Digital Threats, Gendered Realities: Online Harassment in India.* CIS India.
4. Fineman, M. A. (2008). The Vulnerable Subject: Anchoring Equality in the Human Condition. *Yale Journal of Law and Feminism,* 20(1), 1-23.
5. Internet Freedom Foundation. (2023). *Tracking Online Violence against Women in India.* IFF.
6. MacKinnon, C. A. (1989). *Toward a Feminist Theory of the State.* Harvard University Press.

7. National Crime Records Bureau. (2024). *Crime in India 2023.* Ministry of Home Affairs, Government of India.
8. National Commission for Women. (2020). *Annual Report 2019-2020.* NCW, Government of India.
9. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).
10. Kalandi Charan Lenka v. State of Odisha, CRLA No. 174 of 2016 (Orissa High Court, 2017).
11. Navtej Singh Johar v. Union of India, (2018) 10 SCC 1 (Supreme Court of India).
12. The Information Technology Act, 2000 (No. 21 of 2000), as amended by The Information Technology (Amendment) Act, 2008. Parliament of India.
13. The Indian Penal Code, 1860 (No. 45 of 1860). Parliament of India.
14. The Criminal Law (Amendment) Act, 2013 (No. 13 of 2013). Parliament of India.
15. Online Safety Act 2023 (c. 50). Parliament of the United Kingdom.
16. Online Safety Act 2021 (Cth). Parliament of Australia.
17. Baxi, U. (2007). *Human Rights in a Posthuman World.* Oxford University Press.
18. Dhanda, A. (2000). Legal Order and Mental Disorder. Sage Publications.
19. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Ministry of Electronics and Information Technology, Government of India.
20. Ghiassi, R. (2022). Algorithmic Discrimination and Women's Safety Online. *Journal of Cyberpsychology, Behavior, and Social Networking,* 25(4), 211-225.