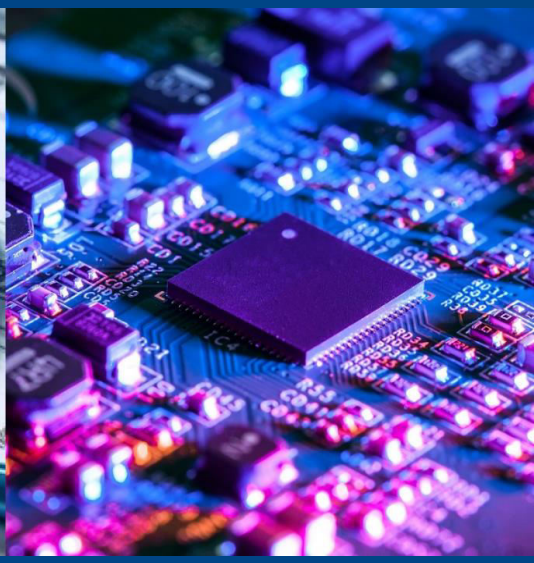
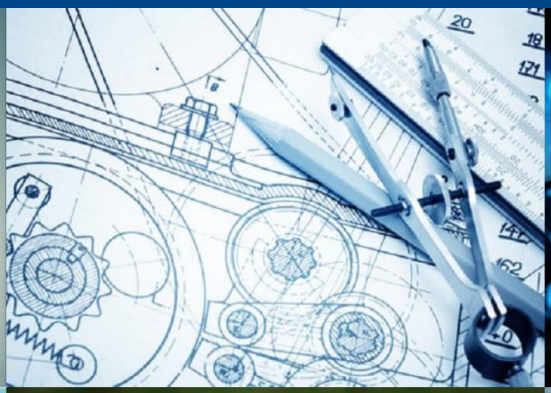
ISSN: 2582-7219

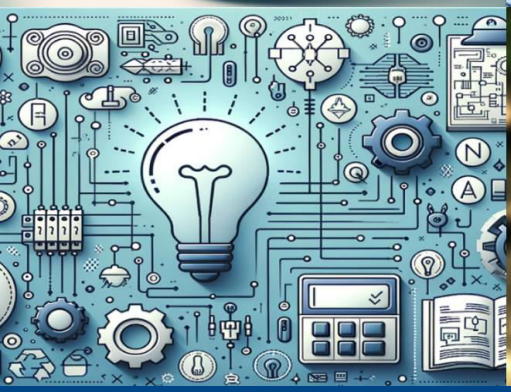




# International Journal of Multidisciplinary Research in Science, Engineering and Technology

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*



**Impact Factor: 7.521**

**Volume 8, Issue 1, January 2025**

© 2025 IJMRSET | Volume 8, Issue 1, January 2025| DOI: 10.15680/IJMRSET.2025.0801061

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

# Public Awareness and Legal Reforms for Combating Revenge Porn and Deepfake Pornography in India's Digital Age

**Saloni Shashank Patil, Dr. S.P. Mishra**

Ph. D Research Scholar, Department of Law, Chhatrapati Shivaji, Maharaj University, Panvel, Navi Mumbai, India

Professor and HOD, Department of Law, Chhatrapati Shivaji Maharaj University, Panvel, Navi Mumbai, India

**ABSTRACT:** The rapid expansion of digital platforms in India has intensified the prevalence of revenge porn and deepfake pornography, posing severe threats to privacy, dignity, and gender equality, particularly for women. The existing legal framework, including the Information Technology (IT) Act, 2000, and Indian Penal Code (IPC), 1860, struggles to address these cybercrimes due to inadequate specificity and enforcement challenges, compounded by socio-cultural barriers like victim-blaming and patriarchal norms. This research paper examines the role of public awareness and legal reforms in combating revenge porn and deepfake pornography, analyzing provisions like IT Act Sections 66E, 67, and IPC Sections 354C, 509. It explores judicial interpretations, such as Avnish Bajaj v. State (2005), and the impact of awareness campaigns in reducing stigma. Drawing on a socio-legal approach, the paper proposes targeted legal reforms, enhanced enforcement, and public education strategies, informed by international frameworks like CEDAW and the UK's Sexual Offences Act, 2003, to align with constitutional guarantees under Articles 14 and 21, fostering a safer digital environment.

**KEYWORDS:** Revenge Porn, Deepfake Pornography, Public Awareness, Legal Reforms, Information Technology Act, Indian Penal Code, Gender Equality, Privacy, Cybercrime, Victim-Blaming.

## I. INTRODUCTION

The rise of digital technologies in India has amplified the threats of revenge porn and deepfake pornography, cybercrimes that violate privacy, dignity, and gender equality, disproportionately affecting women. These issues challenge the legal framework, primarily the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, which lack specificity for addressing manipulated media and non-consensual imagery. Socio-cultural factors, such as patriarchal norms and victim-blaming, exacerbate these challenges, deterring victims from seeking justice and perpetuating harm. This research paper examines the role of public awareness and legal reforms in combating revenge porn and deepfake pornography, analyzing provisions like IT Act Sections 66E and 67, and IPC Sections 354C and 509, alongside judicial decisions like Avnish Bajaj v. State (2005). It explores how awareness campaigns can reduce stigma and empower victims, while assessing enforcement gaps and socio-cultural barriers. Drawing on a socio-legal approach, the paper proposes targeted legal reforms, enhanced enforcement, and public education strategies, informed by international standards like CEDAW and the UK's Sexual Offences Act, 2003, to align with constitutional guarantees under Articles 14 and 21. The objectives are to evaluate current laws, assess awareness initiatives, and recommend measures to foster a safer digital environment.

## II. LEGAL FRAMEWORK ADDRESSING REVENGE PORN AND DEEPFAKE PORNOGRAPHY

India's legal framework for combating revenge porn and deepfake pornography primarily relies on the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, which aim to protect privacy and dignity while addressing cybercrimes within the constitutional mandates of equality (Article 14), privacy, and personal liberty (Article 21). These laws, including IT Act Sections 66E, 67, and 67A, and IPC Sections 354C, 509, and 292, seek to curb the dissemination of non-consensual intimate imagery and obscene content, but their effectiveness is limited by gaps in addressing emerging technologies like deepfakes and socio-cultural challenges such as victim-blaming. Socio-legal analyses emphasize that these legal provisions struggle to keep pace with the rapid evolution of digital platforms,

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

necessitating reforms to ensure robust victim protection. This section examines the key provisions of the IT Act and IPC, their alignment with constitutional principles, and their limitations in tackling revenge porn and deepfake pornography, providing a foundation for analyzing the role of public awareness and judicial responses.

The Information Technology Act, 2000, provides a framework for addressing cybercrimes through Sections 66E, 67, and 67A. Section 66E penalizes the intentional transmission of private images without consent, directly applicable to revenge porn, with penalties up to three years' imprisonment and fines. Sections 67 and 67A target obscene and sexually explicit content, respectively, carrying similar penalties, and can be applied to explicit deepfake material. Section 79 imposes intermediary liability on platforms for failing to remove harmful content, as clarified in Avnish Bajaj v. State (2005), where the court addressed the sale of a non-consensual video. However, these provisions lack specific definitions for deepfake technology, limiting their applicability to manipulated media and creating enforcement challenges in the digital age.

The Indian Penal Code, 1860, complements the IT Act with provisions like Section 354C (voyeurism), introduced in 2013, which criminalizes capturing or disseminating private images without consent, directly addressing revenge porn with penalties up to three years' imprisonment. Section 509 penalizes acts outraging a woman's modesty, while Section 292 addresses obscene content, both applicable to non-consensual imagery but outdated for deepfake contexts. Socio-legal studies note that these provisions, while progressive, fail to account for the synthetic nature of deepfakes, restricting their effectiveness against technologically advanced cybercrimes and leaving victims, particularly women, vulnerable to continued harm.

Constitutional guarantees under Article 14 (equality before law) and Article 21 (right to life, privacy, and dignity) provide the legal foundation for these laws. Article 19(2) allows restrictions on free speech to protect public decency, supporting measures against obscene content. Judicial interpretations, such as those affirming privacy rights, underscore the need to protect victims from digital violations. However, socio-cultural stigma and patriarchal norms deter reporting, undermining constitutional protections. The absence of deepfake-specific provisions and limited platform accountability further weaken the framework's ability to address modern cybercrimes.

The limitations of these laws include their lack of specificity for deepfake pornography, inadequate enforcement mechanisms, and failure to address socio-cultural barriers like victim-blaming, which discourage legal recourse. The next section will explore the socio-cultural context and challenges, analyzing how these factors amplify the harm of revenge porn and deepfake pornography and hinder effective legal implementation.

## III. SOCIO-CULTURAL CONTEXT AND CHALLENGES

The proliferation of revenge porn and deepfake pornography in India is deeply influenced by socio-cultural factors that amplify their prevalence and impact, creating significant challenges for the enforcement of the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860. Patriarchal norms, victim-blaming culture, and gender-based stigma shape societal attitudes toward these cybercrimes, disproportionately affecting women and undermining constitutional guarantees of equality (Article 14) and dignity (Article 21). Socio-legal analyses emphasize that these cultural dynamics deter victims from seeking justice, exacerbate harm through digital platforms, and complicate legal implementation. This section examines the key socio-cultural influences—patriarchal norms and victim-blaming, the role of digital platforms and social media, and socio-economic barriers like digital literacy and access disparities—analyzing their impact on revenge porn and deepfake pornography and their implications for legal enforcement.

Patriarchal norms and victim-blaming culture are central to the perpetuation of revenge porn and deepfake pornography, as they disproportionately target women, reinforcing gender inequalities. Indian society's patriarchal structure often stigmatizes women's sexuality, blaming victims for non-consensual imagery rather than perpetrators, which discourages reporting under IT Act Section 66E or IPC Section 354C. Socio-legal studies highlight that this culture, rooted in traditional gender roles, aligns with practices like dowry, further marginalizing women and violating Article 14's equality mandate. Victims face social ostracism, as seen in cases like Avnish Bajaj v. State (2005), where societal attitudes hindered legal recourse, reducing conviction rates and perpetuating harm.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Digital platforms and social media amplify the impact of these cybercrimes by enabling rapid, anonymous dissemination of non-consensual content. The accessibility of early social media and video-sharing platforms facilitates the spread of revenge porn, with perpetrators exploiting anonymity to evade accountability under IT Act Sections 67 and 67A. Online misogyny, fueled by cultural biases, drives the creation and sharing of deepfake pornography, targeting women to reinforce patriarchal control. Socio-legal analyses note that platforms' failure to enforce intermediary liability under Section 79, despite judicial directives, exacerbates victims' trauma, highlighting the need for stronger content moderation to address these digital-age challenges.

Socio-economic barriers, including limited digital literacy and access to technology, further complicate the response to these cybercrimes. Rural and marginalized communities, with restricted access to internet and smartphones, lack awareness of legal protections, increasing vulnerability to exploitation. Conversely, urban populations with greater technology access face higher exposure to deepfake creation tools, as socio-legal studies indicate. Low digital literacy among victims and law enforcement hinders effective use of IT Act provisions, while economic dependence on male family members discourages women from pursuing legal action, undermining Article 21's right to dignity.

These socio-cultural and socio-economic factors—patriarchal norms, digital platform dynamics, and access disparities—create formidable barriers to addressing revenge porn and deepfake pornography, limiting the efficacy of legal frameworks. The next section will explore the role of public awareness in combating these cybercrimes, analyzing its impact on reducing stigma and encouraging legal recourse.

## IV. ROLE OF PUBLIC AWARENESS IN COMBATING CYBERCRIMES

Public awareness plays a critical role in addressing revenge porn and deepfake pornography in India, as these cybercrimes are amplified by socio-cultural factors like patriarchal norms, victim-blaming, and gender stigma, which deter victims from seeking justice under the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860. By educating communities about legal protections, digital consent, and the harms of non-consensual imagery, awareness campaigns can reduce stigma, empower victims, and enhance enforcement of laws like IT Act Sections 66E, 67, and IPC Section 354C. Socio-legal analyses emphasize that public awareness is essential to counter cultural barriers and support constitutional guarantees of equality (Article 14) and dignity (Article 21). This section examines current awareness initiatives, their impact on reducing stigma and encouraging reporting, and the limitations posed by socio-cultural resistance and limited outreach, particularly in rural areas.

Current awareness initiatives in India, led by NGOs, government bodies, and media, have sought to educate the public about cybercrimes and legal rights. Organizations like the Human Rights Law Network have conducted workshops on digital privacy, highlighting protections under the IT Act and IPC, as seen in campaigns addressing online harassment. Government efforts, such as cybercrime awareness programs by the Ministry of Home Affairs, aim to inform citizens about reporting mechanisms under Section 66E for privacy violations. Media outlets, including print and television, have occasionally covered cases like Avnish Bajaj v. State (2005), raising awareness about intermediary liability and victim rights. These initiatives aim to shift societal attitudes by challenging victim-blaming narratives and promoting gender equality.

The impact of these campaigns is evident in increased reporting of cybercrimes, particularly in urban areas, where awareness of IT Act provisions has empowered some victims to seek legal recourse. Socio-legal studies note that public education reduces stigma, encouraging women to report non-consensual imagery under IPC Section 354C, as stigma often deters victims due to fear of social ostracism. Campaigns highlighting the psychological and social harm of revenge porn have fostered empathy, aligning with Article 21's dignity mandate. In select cases, media coverage has pressured platforms to remove harmful content, reinforcing Section 79's intermediary liability and supporting victims' access to justice.

However, limitations persist due to socio-cultural resistance and inadequate outreach. Rural areas, with limited access to media and digital literacy, remain underserved, as socio-legal analyses highlight, leaving marginalized women vulnerable to exploitation without awareness of legal protections. Patriarchal norms and victim-blaming, deeply rooted in societal attitudes, resist change, as seen in low conviction rates under IPC Section 509. The absence of deepfake-specific awareness, given the technology's novelty, further limits campaign effectiveness, as public understanding of

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

manipulated media remains low. These gaps hinder the reduction of stigma and reporting in rural and conservative communities.

Addressing these limitations requires sustained, targeted awareness efforts to complement legal enforcement. The next section will analyze judicial interpretations, examining their role in shaping the response to revenge porn and deepfake pornography and addressing socio-cultural challenges.

## V. JUDICIAL INTERPRETATIONS AND THEIR IMPACT

Judicial interpretations have been pivotal in shaping India's response to revenge porn and deepfake pornography, navigating the legal framework provided by the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, while aligning with constitutional guarantees under Articles 14, 21, and 19(2). Courts have addressed non-consensual intimate imagery, balancing victim protection with free speech and privacy rights, amidst socio-cultural challenges like patriarchal norms and victim-blaming. Socio-legal analyses highlight the judiciary's role in clarifying legal provisions, yet limitations persist due to the absence of deepfake-specific precedents. This section examines key judicial decisions, such as Avnish Bajaj v. State (2005), their impact on combating these cybercrimes, judicial trends recognizing privacy under Article 21, and challenges posed by inconsistent rulings, providing insights into their role in addressing socio-cultural barriers.

In Avnish Bajaj v. State (2005), the Delhi High Court addressed intermediary liability under Section 79 of the IT Act, involving the sale of a non-consensual intimate video on an online platform. The court held that intermediaries could face liability for failing to remove obscene content, aligning with Section 67 and Article 19(2)'s restrictions on free speech for public decency. This ruling set a precedent for platform accountability, emphasizing victim protection and countering socio-cultural victim-blaming by prioritizing legal recourse. However, it did not address deepfake technology, reflecting a gap in judicial capacity to tackle emerging cybercrimes, limiting its applicability to manipulated media.

Judicial trends have increasingly recognized privacy and dignity as fundamental rights under Article 21, particularly for women victims of non-consensual imagery. Courts have applied IPC Section 354C (voyeurism) and Section 509 (outraging modesty) to address revenge porn, reinforcing Article 14's equality mandate by protecting victims from gender-based harm. Socio-legal studies note that these rulings, while progressive, are constrained by the lack of deepfake-specific precedents, as synthetic media requires technical expertise beyond existing provisions. Judicial efforts to uphold privacy have encouraged reporting, but societal stigma continues to deter victims, reducing the impact of these interpretations.

Challenges include inconsistent lower court rulings and the absence of deepfake-focused judgments. Lower courts often vary in applying IT Act Sections 66E and 67, leading to delays and uneven justice delivery, as socio-legal analyses highlight. The novelty of deepfake technology, not addressed in cases like Avnish Bajaj, limits judicial effectiveness, as courts rely on outdated provisions. Socio-cultural resistance, including victim-blaming, further complicates judicial outcomes, as victims face social pressure when seeking redress, undermining Article 21's dignity protections.

These judicial interpretations have advanced victim protections by clarifying platform liability and privacy rights but are limited by legal gaps and societal attitudes. The next section will propose legal reforms and public awareness strategies to address these challenges, fostering a comprehensive response to revenge porn and deepfake pornography.

## VI. PROPOSED REFORMS AND AWARENESS STRATEGIES

India's legal framework, encompassing the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, struggles to combat revenge porn and deepfake pornography due to legal gaps, enforcement challenges, and socio-cultural barriers like victim-blaming and patriarchal norms. These issues undermine constitutional guarantees of equality (Article 14) and privacy (Article 21), necessitating robust reforms and public awareness strategies. Socio-legal analyses highlight the need for targeted legislation, enhanced enforcement, and education to address these cybercrimes effectively. Drawing on international models like the UK's Sexual Offences Act, 2003, and CEDAW principles, this section proposes legislative reforms, strengthened enforcement mechanisms, public awareness campaigns,

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

technological interventions, and alignment with international standards to foster a comprehensive response to revenge porn and deepfake pornography in India's digital landscape.

Legislative reforms are essential to address the lack of specific provisions for deepfake pornography and revenge porn. Enacting a dedicated law, inspired by the UK's Sexual Offences Act, 2003, with clear definitions of non-consensual intimate imagery and synthetic media, would strengthen prosecutions under Article 21's privacy protections. Amending the IT Act to include provisions for deepfake technology under Section 66E and increasing penalties for Sections 67 and 67A violations would deter offenders. Updating IPC Section 354C to cover manipulated content, as noted in socio-legal studies, would address gaps seen in Avnish Bajaj v. State (2005), ensuring legal clarity and victim redress.

Strengthening enforcement requires establishing specialized cybercrime units and training law enforcement in digital forensics, addressing the expertise gap highlighted in socio-legal analyses. These units, modeled on UK practices, would enhance prosecution rates under IT Act provisions. Creating victim support systems, including counseling and legal aid, as mandated by Article 21's dignity principle, would encourage reporting despite socio-cultural stigma. Regular audits of online platforms, enforcing Section 79 intermediary liability, would ensure swift removal of harmful content, reducing victim trauma.

Public awareness campaigns are crucial to counter victim-blaming and gender stigma. Educational initiatives via media, including television and print, should inform communities about legal protections under the IT Act and IPC, reducing shame for women victims, as seen in Avnish Bajaj. NGO-led workshops on digital consent and privacy, aligned with CEDAW's Article 5, would challenge patriarchal norms, empowering victims to seek justice. These campaigns would address low reporting rates by fostering empathy and aligning with Article 14's equality mandate.

Technological interventions, such as mandating AI-based content moderation on platforms to detect deepfakes, would enhance accountability. Regulations requiring user identity verification for explicit content uploads, inspired by global practices, would curb anonymity-driven offenses. These measures would complement IT Act enforcement, addressing the rapid spread of non-consensual imagery. The next section will conclude the analysis, summarizing findings and outlining a future outlook for combating these cybercrimes.

## VII. CONCLUSION

India's response to revenge porn and deepfake pornography, governed by the Information Technology (IT) Act, 2000, and the Indian Penal Code (IPC), 1860, is hindered by legal gaps, enforcement challenges, and socio-cultural barriers such as victim-blaming and patriarchal norms, undermining constitutional guarantees of equality (Article 14) and privacy (Article 21). Judicial interpretations, like Avnish Bajaj v. State (2005), have clarified platform liability and privacy rights, but the absence of deepfake-specific provisions limits their impact. Socio-legal analyses highlight that public awareness campaigns, though limited, have begun to reduce stigma, yet socio-cultural resistance and technological advancements continue to exacerbate harm. The comparative analysis with the UK's Sexual Offences Act, 2003, and CEDAW principles underscores the need for targeted legislation and robust enforcement. Proposed reforms—enacting specific laws, strengthening cybercrime units, launching awareness campaigns, and implementing technological interventions—offer a comprehensive strategy to address these gaps. These measures aim to empower victims, reduce gender-based stigma, and ensure platform accountability, aligning with constitutional mandates. The future of combating these cybercrimes in India's digital landscape depends on integrating legal reforms with sustained public education, fostering a society that upholds dignity, equality, and justice for all.

## REFERENCES

1. Avnish Bajaj v. State. (2005) 3 Comp LJ 364 Del.
2. Bandewar, Sunita. "Abortion Services and Providers' Perceptions: Gender Dimensions." Economic and Political Weekly, vol. 38, no. 21, 2003, pp. 2075-2081.
3. Basu, Durga Das. Shorter Constitution of India. 14th ed., LexisNexis, 2011.
4. Baxi, Upendra. "Abortion and the Law in India." Journal of the Indian Law Institute, vol. 28-29, 1986-87, pp. 28-29.
5. Berlatsky, Noah. Abortion. Greenhaven Press, 2011.
6. Centre for Enquiry into Health and Allied Themes (CEHAT) v. Union of India. (2001) 5 SCC 577.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

7. Chitnis, Varsha, and Danaya Wright. "The Legacy of Colonialism: Law and Women's Rights in India." Washington & Lee Law Review, vol. 64, no. 4, 2007, pp. 1315-1348.
8. Constitution of India, 1950. Government of India, 1950.
9. D. Rajeshwari v. State of Tamil Nadu. 1996 Cri LJ 3795.
10. Dasgupta, Suprio. "The Right to Abortion." Lawyers Collective, vol. 9, 1994, pp. 16-18.
11. Dr. Nikhil Dattar v. Union of India. Writ Petition No. 1816 of 2008, Bombay High Court, 2008.
12. Gaur, K.D. "Cyber Laws in India: An Overview." Journal of the Indian Law Institute, vol. 49, no. 2, 2007, pp. 201-220.
13. Government of India. Census of India 2001: Sex Ratio. Office of the Registrar General & Census Commissioner, 2001.
14. Halder, Debarati, and K. Jaishankar. "Revenge Porn by Teens in the United States and India: A Socio-Legal Analysis." International Journal of Cyber Criminology, vol. 5, no. 2, 2011, pp. 857-865.
15. Indian Penal Code, 1860. Government of India, 1860.
16. Information Technology Act, 2000. Government of India, 2000.
17. Jain, M.P. Indian Constitutional Law. 6th ed., LexisNexis Butterworths, 2011.
18. Jaiswal, J.V.N. Legal Aspects of Pregnancy, Delivery, and Abortion. Eastern Book Company, 2009.
19. Jesani, Amar, and Aditi Iyer. "Women and Abortion." Economic and Political Weekly, vol. 27, no. 46, 1992, pp. 2467-2470.
20. Kamdar, Mira. Cyberlaw in India. Universal Law Publishing, 2009.
21. Medical Termination of Pregnancy Act, 1971. Government of India, 1971.
22. Medical Termination of Pregnancy (Amendment) Act, 2002. Government of India, 2002.
23. Murari Mohan Koley v. The State. 2003 Cri LJ 1482.
24. National Crime Records Bureau. Crime in India 2010. Ministry of Home Affairs, Government of India, 2010.
25. Paranjape, V.N. Indian Penal Code. Central Law Publications, 2010.
26. Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 2002. Government of India, 2002.
27. "Reproductive Rights in India." Human Rights Law Network, hrln.org/hrln/training-and-development/about-ccri/433.html. Accessed 9 June 2011.
28. United Nations. Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). United Nations, 1979.
29. United Nations. Beijing Declaration and Platform for Action. Fourth World Conference on Women, 1995.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

# INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

## IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com