myresearchgo

myresearchgo Volume 2, Issue 5, May 2026, ISSN: 3107-3816 (Online)

Doxing as Digital Violence: Gender, Power and the Silencing of Dissent

Dr. Jennifer Coutinho,

Associate Professor,

Department of Sociology, Ratnam College, Mumbai;

Email: coutinhojennifer21@gmail.com;

Mobile: +91 982 052 7961

Abstract

In an increasingly networked world, the boundary between online interaction and offline safety is rapidly eroding. What begins as a post, tweet or coordinated digital attack can quickly escalate into harassment, fear and tangible harm. Among the most concerning manifestations of this shift is *doxing*—the non-consensual disclosure of personal information to intimidate, shame or silence individuals.

Far from being a fringe phenomenon, doxing has emerged as a pervasive form of digital violence that disproportionately targets women, minorities and those who challenge dominant political or social narratives.

Drawing on feminist theory, Foucauldian notions of power and surveillance, and scholarship on digital cultures; the paper argues that doxing must be understood as a structural and gendered form of violence. It examines how personal data is mobilised to regulate visibility and suppress dissent, while also highlighting gaps in legal frameworks and platform accountability. By situating doxing at the intersection of gender, power and digital culture, the paper calls for a survivor-centric response that integrates legal reform, institutional responsibility and recognition of lived experiences in digital spaces.

Keywords: Doxing, digital violence, gender-based cybercrime, surveillance, power, online harassment, platform accountability

Introduction

In early 2022, a disturbing episode of online abuse shook public consciousness in India. Dozens of Muslim women—journalists, students, activists, and professionals—discovered that their photographs had been extracted from public platforms and uploaded onto an application called *Bulli Bai*, where they were subjected to a degrading "auction."

While the incident was widely condemned, it also revealed something deeper about the nature of digital violence. The harm was not only symbolic but structural: it relied on the systematic exposure, circulation and amplification of personal data in ways that made targeted individuals feel unsafe both online and offline.

Although such cases do not always fit neatly into technical definitions of doxing, they operate through similar logics—where visibility is weaponised and personal information becomes a tool of intimidation. This paper argues that doxing must be understood as a form of digital violence embedded in broader systems of gendered power, surveillance and political control.

Understanding Doxing

The term *doxing* refers to the non-consensual publication of personal information online (Douglas, 2016). It collapses the boundary between digital and physical spaces, exposing individuals to risks that extend beyond the internet.

It typically manifests in three forms:

- **De-anonymising doxing** – revealing identities
- **Targeting doxing** – exposing private data
- **Delegitimising doxing** – undermining credibility

Theoretical Framework: Power, Surveillance and Gendered Digital Violence

Three theoretical lenses address doxing not just as individual acts of harassment but as part of structures that enable and sustain it:

1. Doxing as Surveillance and Disciplinary Power

In *Discipline and Punish*, Foucault (1977) describes how modern power operates not through overt force, but through surveillance and the internalisation of control.

In this sense, doxing produces what Foucault might describe as *self-regulating subjects*: individuals who withdraw from public discourse out of fear of exposure. The power of doxing lies less in the data itself and more in its ability to create a climate of constant vulnerability.

2. Feminist Perspectives: Patriarchy and the Regulation of Visibility

Feminist scholars have long argued that public visibility for women is fraught with risk. The digital sphere, rather than being emancipatory, often reproduces patriarchal structures (Citron, 2014). Doxing operates as a gendered practice because it disproportionately targets women who are visible, vocal or transgressive. It functions as a form of *gendered policing*, punishing women who step outside prescribed social roles. Online abuse often reflects deeply embedded misogyny, where women's participation in public discourse is met with hostility and attempts at silencing.

Anita Sarkeesian, a Canadian-American feminist media critic who created a web series examining misogyny in video games, is among the most well-known examples of the gendered impact of doxing. Sarkeesian experienced severe persecution after her work was published, including death threats, doxing and swatting—

a hoax that resulted in armed police visiting her residence (Chess & Shaw, 2015). This situation is not exceptional; according to Amnesty International (2018), doxing is a prelude to stalking, losing one's work or residence and women around the world experience coordinated online abuse that frequently develops into real-world safety hazards.

The intersectional dimension is equally critical. Women from marginalised communities—such as Muslim women in the *Bulli Bai* case—face layered forms of violence shaped by religion, caste and identity (Crenshaw, 1991). Doxing in such contexts is not merely misogynistic but also communal and political.

3. Platform Power and Networked Harassment

From a digital sociology perspective, doxing must also be understood within the architecture of online platforms. Social media platforms operate through what van Dijck (2013) calls the *logic of connectivity*, where visibility, engagement and virality are central.

These systems can amplify harm. Algorithms that prioritise engagement may inadvertently promote abusive content, while anonymity lowers barriers to participation in harassment campaigns. As Citron and Franks (2020) argue, the design of platforms often enables coordinated abuse while diffusing accountability.

Doxing, therefore, is not just an individual act but part of a *networked phenomenon*, where multiple actors participate in the circulation and amplification of harm.

Doxing and the Silencing of Dissent

Doxing is frequently used to target journalists, activists and dissenters. The case of Rana Ayyub demonstrates how personal information can be weaponised to intimidate and discredit (OHCHR, 2022). Coordinated smear campaigns, altered photos and violent threats are all examples of the harassment that she faced. Similarly, women involved in movements such as #MeToo or anti-CAA protests have faced coordinated exposure and harassment (Scroll, 2018; The Wire, 2020).

These patterns reveal that doxing is not random—it is a political strategy aimed at suppressing dissent. By making participation unsafe, it narrows the scope of democratic engagement.

Platform Accountability

Whether through carelessness or insufficient security, social media companies and internet service providers have contributed to the growth of doxing. While reporting procedures are usually ambiguous and ineffectual, algorithms that incentivize viral posts frequently intensify harassment campaigns (Citron & Franks, 2020). These platforms frequently fail to take prompt action to eliminate dangerous content, leaving the victim to bear the responsibility for responding. Even while Reddit, Facebook, and Twitter have amended their policies against harassment, enforcement is still uneven. 84% of reported abusive tweets directed at women persisted online after being flagged, according to a report by the Center for Countering Digital Hate. These mistakes point to a structural problem: platform design puts profit and viewer engagement ahead of user safety, especially for disadvantaged groups.

The Law and legal policy gaps

In India a few cases of doxing managed to reach the Courts:

- The Odisha High Court in Subhranshu Rout @ Gugul v. State Of Odisha (2020) expressed that due to the lack of specific legal provisions, the courts cannot adopt a gender-sensitive approach to doxing by addressing the privacy concern it raises. In this case, the photos and videos of a rape victim were uploaded online by creating a fake Facebook account. The court noted that India's sentencing-oriented criminal justice system is not adequate to address the privacy infringement suffered by the victim, as it does not recognize the right to be forgotten and does not contain provisions for getting photos erased from the server of the social media platforms permanently.

- In another case that made it to the Delhi High Court in 2021 (X v. https://www.youtube.com/watch?v=iq6k5z3zys0), involved a film director who had recorded some video footage of an actress and offered her a starring role in return. He later posted these recordings on his YouTube account, unrelated to the film and without her knowledge or approval. In this case as well, the court appropriately acknowledged the privacy concern at hand and maintained the petitioner's right to be free from unwelcome invasions of her privacy by third parties due to the publicly available footage. The court's judgment mandated that the defendants take down the video from the YouTube channel and instructed search engines to take down the video from their listings and search results sites.

- In a civil suit (Ms. Nimisha Bhagat v. Sneha Mahajan Nee Dogra @ Sneeha) in 2020 before a Delhi Court, a compensation was awarded to the petitioner for the acts of the defendant who posted provocative, derogative and threatening comments against her on Facebook and WhatsApp groups and circulated her phone numbers to strangers who then proceeded to troll the petitioner.

Doxing is not explicitly recognised as a standalone offence in India. Instead, it is addressed through fragmented provisions related to privacy, stalking and defamation.

In the Indian context, certain provisions offer partial remedies. For instance, cyberstalking may be prosecuted under Section 354D of the Indian Penal Code (now Section 78 of the Bharatiya Nyaya Sanhita, 2023), while violations involving images may fall under Section 66E of the Information Technology Act or voyeurism-related provisions. Similarly, Sections 43 and 72 of the IT Act address breaches of confidentiality and privacy. However, these laws are primarily framed in terms of individual offences or economic harm and do not adequately recognise doxing as a form of targeted, gendered and often collective harassment.

Judicial interventions have, at times, attempted to bridge these gaps by foregrounding privacy concerns and the right to dignity. Yet, as seen in cases such as Subhranshu Rout v. State of Odisha (2020), courts themselves have acknowledged the limitations of existing legal provisions, particularly in addressing issues like the right to be forgotten and the permanent removal of harmful content from digital platforms. The Information Technology (Intermediary Liability and Digital Media Ethics Code) Rules, 2021 provide an additional mechanism by enabling courts to direct intermediaries to remove content that violates privacy.

Conclusion

Doxing represents a convergence of surveillance, patriarchy and platform power. It transforms personal data into a tool of control, reinforcing existing inequalities while creating new forms of vulnerability.

Addressing doxing requires a structural response. Legal frameworks must explicitly recognise it as a form of harm. Platforms must be held accountable for the environments they create. At the same time, there must be greater recognition of the lived realities of those affected. Ultimately, the question is not only how to regulate digital spaces, but how to ensure that they remain open, inclusive and safe for participation.

References

1. Amnesty International. (2018). *Toxic Twitter: A toxic place for women*.
2. Chess, S., & Shaw, A. (2015). A conspiracy of fishes. *Journal of Broadcasting & Electronic Media*, 59(1).
3. Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.
4. Citron, D. K., & Franks, M. A. (2020). The internet as a speech machine.
5. Crenshaw, K. (1991). Mapping the margins: Intersectionality. *Stanford Law Review*.
6. Douglas, M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*.
7. Duggan, M. (2017). *Online harassment 2017*. Pew Research Center.
8. Foucault, M. (1977). *Discipline and punish: The birth of the prison*.
9. Gillespie, T. (2018). *Custodians of the internet*. Yale University Press.
10. Jane, E. A. (2017). *Misogyny online*. SAGE.
11. OHCHR. (2022). *UN experts call on India to stop targeting journalist Rana Ayyub.* Retrieved from https://www.ohchr.org/en/press-releases/2018/05/un-experts-call-india-protect-journalist-rana-ayyub-online-hate-campaign?LangID=E&NewsID=23126
12. Zahid A (2025): For women journalists, systematic abuse and trolling is a familiar story across borders. *Scroll.in* Retrieved from https://scroll.in/article/1080739/for-women-journalists-systematic-abuse-and-trolling-is-a-familiar-story-across-borders
13. Van Dijck, J. (2013). *The culture of connectivity*. Oxford University Press.
14. L. C. Kasireddy, L. Popuri, G. Karunanithi, A. Varghese, S. Ahamad and Dharamvir, "Securing Business Data in Multi-Cloud Environments," 2025 International Conference on Digital

Innovations for Sustainable Solutions (ICDISS), Faridabad, India, 2025, pp. 1-6, doi: 10.1109/ICDISS68238.2025.11320589.

15. L. C. Kasireddy, S. Paruchuri, C. Janakamma, A. Sarawat, K. C. Ravi and R. Kumar Chandu, "Cloud-Oriented IoT: Distributed Power-Aware Security Scheme with Data Integrity and Performance Enhancement," 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199185

16. L. C. Kasireddy, A. Jeraldine Viji, P. K. Sholapurapu, D. Sowjanya Kolluru, D. U. Vishweshwar and P. Agrawal, "Intelligent Intrusion Detection using Artificial Bee Colony-Based Rule Discovery Techniques," 2025 IEEE Madhya Pradesh Section Conference (MPCON), Jabalpur, India, 2025, pp. 691-696, doi: 10.1109/MPCON66082.2025.11256592.

17. L. C. Kasireddy, S. Paruchuri, C. Janakamma, A. Sarawat, K. C. Ravi and R. Kumar Chandu, "Cloud-Oriented IoT: Distributed Power-Aware Security Scheme with Data Integrity and Performance Enhancement," 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199185.

18. J. L., L. Chandrakanth Kasireddy, R. V. Palanivel, G. Sushma, K. Bhimaavarapu and P. V. Reddy, "Predictive Modeling in Economics: The Role of AI and Deep Learning," 2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS), Indore, India, 2025, pp. 1-7, doi: 10.1109/WorldSUAS66815.2025.11199198

19. N. Soni, L. C. Kasireddy, T. S., C. Sinhgadiya, S. Kumar and A. T. S., "A Recurrent Neural Network Framework for Effective DDoS Attack Detection in Cloud Computing," 2025 2nd International Conference on Multidisciplinary Research and Innovations in Engineering (MRIE), Gurugram, India, 2025, pp. 594-598, doi: 10.1109/MRIE66930.2025.11156616.

20. Jadhav, D., & Shinde, C. (2026). Sakhi: Stay safe stay fashionable. myresearchgo, 2(1), 1. https://doi.org/10.64448/myresearchgo.vol2.issue1.01.

21. Jadhav, A. (2026). AI-enhanced employee management system. myresearchgo, 2(1), 8. https://doi.org/10.64448/myresearchgo.vol2.issue1.02.

22. Rane, G., & Matteti, V. (2026). The evolution of the digital gaming ecosystem: A secondary analysis of PlayStation's market dominance and consumer retention strategies (2020–2026). Myresearchgo, 2(3), 1. https://doi.org/10.64448/myresearchgo.vol2.issue3.01.

23. Ansari, N., Sharma, A., & Yadav, S. (2026). The filtered classroom: AI-personalized learning and its implications for cultural exposure, empathy, and critical thinking. Myresearchgo, 2(3), 12. https://doi.org/10.64448/myresearchgo.vol2.issue3.02.

24. Junghare, P., Chheniya, J., Behare, M., Kashte, P., Belekar, S., Dhoble, V., & Kumari, S. (2026). Google's Neural Memory Architecture: A Comprehensive Review of the Titans Framework. Myresearchgo, 2(4), 75. https://doi.org/10.64448/myresearchgo.vol2.issue4.12.