



WEAPONISATION OF PERSONAL DATA AGAINST WOMEN: LEGAL GAPS IN ADDRESSING DOXXING IN INDIA

Hamiya M Sagith*

ABSTRACT

The rapid growth of the digital platforms has led to a spike in technology-facilitated gender-based violence, and doxxing is one of these crimes. Even after a rise in such cases, it is unfortunate that there are no proper and specific laws to tackle them. The disclosure of an individual's information without their consent to weaponise their private details against them, leading women to harassment, humiliation, threats and psychological harm, and this is what doxxing is. This paper critically analyses how the doxxing cases are dealt with till now and examines the existing provisions under the Information Technology Act, 2000 and Bharatiya Nyaya Sanhita, 2023, which are relied upon by the legal system. With the help of cases such as Ritu Kohli, Shaviya Sharma v. Squint Neon,¹ and the Bulli Bai and Sulli Deals incidents, the paper emphasises the recent and frequent violence against women from the marginalised community. This article thoroughly scrutinises anti-doxxing laws in the UK, the US, South Korea, Spain and other jurisdictions and concludes by stating certain remedies that need to be implemented in India for a smooth flow of the justice system.

Keywords: IT Act, 2000, BNS, 2023, South Korea, US, UK.

INTRODUCTION

The growth of digital platforms has transformed cyberspace into a critical arena for social interaction, political expression and professional engagement. However, this transformation has led to a rapid increase in violence, especially against women. The National Cybercrime Reporting Portal (NCRP) has reported that online crime against women has risen from 22,188 in 2020 to 48,475 in 2024, showing a 118.4% increase in the number of such crimes.

*BBA LLB (HONS.), FOURTH YEAR, GOVERNMENT LAW COLLEGE, KOZHIKODE.

¹ *Shaviya Sharma v Squint Neon & Ors* 2024 SCC OnLine Del 1445 (Del HC, 22 February 2024)

Notwithstanding the above, it is also reported that cyber security incidents in India rose from 10.29 lakh in 2022 to 22.68 lakh in 2024.² Over the years, violence against women have escalated³ but the most melancholic fact is that, even though there is a rise in online crime against women, there are no proper and specific laws to tackle most of the cybercrime, especially doxxing.

DOXXING

Doxxing is an offensive act in which a wrong doer, often with a malicious intention, publicizes an individual's personnel information (Address, Telephone number, Aadhar Details, photo without consent, financial details etc) online without their consent which is likely to put that individual through humiliation, terrifying experience, defamation and the person may end up having an unhealthy mental condition.⁴

In the case of Shaviya Sharma vs Squint Neon & Ors.,⁵ Delhi High Court has interpreted doxxing as -

Doxxing comes from the phrase 'dropping document' or 'dropping box' on someone, which appears to have originated in the 1990s, involving uncovering and revealing the identity of people who fostered anonymity. It is further observed that even if doxing is not used as a tool for sexual harassment, these factors also contribute to the harms of having personal information revealed on the Internet, as there is disclosure/ public release of an individual's private, sensitive, personal information.

Doxxing, being a criminal act, violates the Fundamental rights of an individual under Article 14 (Right to Equality) and Article 21 (Right to Dignity and Privacy). In the case, Justice K.S. Puttaswamy (Retd.) v. Union of India,⁶ the Supreme Court held that "privacy is intrinsic to life and personal liberty and is a core of human dignity."

² Press Information Bureau, 'PIB Headquarters' <<https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3®=3&lang=2>> accessed 24 January 2026

³ Shanker N, 'A Legal Analysis of Cyber Child Pornography in India under Information Technology Act, 2000' (2024) 4 *International Journal of Criminal, Common and Statutory Law* 34

⁴ Internet Freedom Foundation, 'Why Doxxing Remains a Legal Grey Area: Navigating the Legal Uncertainty of Online Exposure' <<https://internetfreedom.in/why-doxxing-remains-a-legal-grey-area-navigating-the-legal-uncertainty-of-online-exposure/>> accessed 24 January 2026

⁵ Supra note.1

⁶ *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1 (India) [298]

The Supreme Court in the Auto Shanker case,⁷ has stated that the right to privacy or the right to be let alone is guaranteed by Article 21 of the Indian Constitution. An individual has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education, among other matters.⁸ None can publish anything concerning the above matter without his or her consent, whether truthful or otherwise. If someone does that, they would be violating the fundamental right, right to privacy (Article 21), of that particular person.

CASES OF DOXXING WHERE WOMEN ARE TARGETED AND THE INADEQUATE LAWS

India's first cyber stalking case was reported in 2001, and in this case, an Indian woman named Ms Ritu Kohli was stalked by Manish Kathuria. He used her name and chatted to others in an obscene language on the website, www.mirc.com and distributed her residential telephone number to contact her, as a result of which she received a lot of obscene calls. The case was later filed under Section 509 of IPC, which criminalised words, gestures or acts intended to insult the modesty of a woman.⁹ IPC was drafted for physical-world offences, but over time, IPC (Indian Penal Code) was replaced by (BNS) Bharatiya Nyaya Sanhita. Hence, if we apply BNS, the legal provisions applicable here are Sec 79 of BNS, which covers Insulting the Modesty of a Woman in any form, even through electronic means, Sec 78 of BNS (Cyberstalking) and Sec 356 of BNS (Defamation even in an electronic mode). Additionally, Sections under the Information Technology Act 2000, such as Section 66C (Punishment for Identity Theft), Section 66D (Cheating by Personation), are also applicable here.

But an important point to note here is that, even after Manish Kathuria distributed Ritu Kohli's residence telephone number to the public without her consent the case was not filed under any provision indicating punishment for doxxing and even if we try to apply any existing provision against doxxing we can't find any because no provision penalises Doxxing directly rather, the victims of Doxxing are made to rely on certain provisions of Bharatiya Nyaya Sanhita, 2023 and Information Technology Act, 2000 based on the scenario.

⁷ *R Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632 (SC)

⁸ J N Pandey, *Constitutional Law of India* (60th edn, Central Law Agency 2023)

⁹ J N Pandey, 'The Criminal Law (Amendment) Act, 2013: Legislative Remedies for Online Harassment and Cyberstalking in India' [2016] *SSRN Electronic Journal*

Recently, an article published by the Hindu, a reputable newspaper publication, titled ‘-Stalked, doxxed’: Internet turning into nightmare for Delhi women, has explained a few recent incidents of Doxxing faced by women of Delhi¹⁰ and it further emphasises that the cybercrimes are really high in number, but women refuse to report them as a result of which-

“The National Crime Records Bureau (NCRB) data released recently for 2023 recorded only 36 cybercrimes against women, of which 28 were linked to publishing or transmission of sexually explicit material, and eight were in the category of other women-centric cybercrimes, including blackmail, defamation, morphing and fake profiles.”

Bulli Bai and Sulli Deals cases are the two prominent cases that reflect the gendered Islamophobia in the digital world. In July 2021, Sulli Deals, a website, appeared on GitHub (an Open-Source Platform), and this website placed Muslim women (mainly journalists, activists, students and public figures) on sale or auction by displaying their photographs and personal details. Even though this sale is not real, the number of women targeted was vast. Subsequently, in 2022, another website named Bulli Bai came into the frame with a similar motive to target Muslim women by illegally auctioning them. All of these accused were booked under Sec 153A (now Section 196 of BNS- Promoting enmity between groups), 354D (Now Sec 78 of BNS cyberstalking), Section 509 (Now Sec 79 of BNS word, gesture or act intended to insult the modesty of a woman), Section 500 (Now Section 356 of BNS, criminal defamation) of the Indian Penal Code and Section 67 (publishing or transmitting obscene material in electronic form) of the Information Technology Act, 2000.¹¹

Other than the above-mentioned fragmented and ambiguous laws, the other laws that can be relied on by victims of Doxxing include –

Sec 77 BNS (Voyeurism), Sec 66E of IT Act (violation of privacy), Sections 67 (Punishment for publishing or transmitting obscene material in electronic form) and 67A of IT Act (Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form). On the same hand, the Digital Personal Data Protection Act, 2023, marks a significant step towards recognising the sensitivity of intimate personal data; its enforcement framework remains constrained by an expansive “publicly available” exception, which

¹⁰ A Butani, “‘Stalked, Doxxed’: Internet Turning into Nightmare for Delhi Women’ *The Hindu* (Delhi, 2 December 2025) <<https://www.thehindu.com/news/cities/Delhi/stalked-doxxed-internet-turning-into-nightmare-for-delhi-women/article70346992.ece>> accessed 24 December 202

¹¹ Supra note.10

undermines meaningful consent and permits the weaponisation of personal information through non-consensual republication.

The Committee on the Elimination of Discrimination against Women acknowledges that gender-based violence may affect some women to different degrees, or in different ways, meaning that appropriate legal and policy responses are needed.¹²

LAWS OF OTHER COUNTRIES THAT CAN BE REFERRED TO MAKE UP AN ANTI-DOXXING LAW IN INDIA

The UK have adopted the Data Protection Act, 2018 (DPA,2018), which states that if an individual needs to be legally identified, then a court order signed by a judge must be issued to the ISP. Section 1 of the Protection from Harassment Act, 1997, emphasises that if a person engages in an activity and they have reasonable grounds to believe that the act constitutes harassment, then it is an offence. The provision of the Malicious Communications Act 1988 has enabled the coverage of ‘revenge porn’. Section 127 of the Communication Act, 2003 states that if a person sends a message that is grossly offensive, indecent, obscene or menacing in nature through electronic means, then the person would be deemed to have committed a crime. The Computer Misuse Act 1990 has certain provisions that address doxxing.¹³

Singapore have adopted the Protection from Harassment Act (POHA),1997 to deal with doxxing. Sections 3 and 5 deal with holding a person guilty for publishing personal information of another individual without their consent in order to cause harassment and distress to the other person.¹⁴ According to a study by the Australian Institute in 2019, nearly 5% of Australian Citizens have experienced doxxing, and as a result, the Australian Government has introduced laws such as State and Territory laws targeting stalking behaviours, as well as Federal laws designed to tackle online harassment.¹⁵

¹² CEDAW, *General Recommendation No 28 on the Core Obligations of States Parties under Article 2 of the Convention on the Elimination of All Forms of Discrimination against Women* (16 December 2010) UN Doc CEDAW/C/GC/28, para 18

CEDAW, *Report of the Inquiry concerning Canada under Article 8 of the Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women* (6 March 2020) UN Doc CEDAW/C/OP.8/CAN/1, para 197

¹³ Nihitha PK, ‘Doxxing Celebrities: Addressing Legal Gaps and Proposing Reforms in India’ (2025) 13(1) *International Journal for Scientific Research & Development*

¹⁴ Supra note.13

¹⁵ Lexology, ‘Doxxing Laws Australia?’ < <https://www.lexology.com/library/detail.aspx?g=8b6c8122-e728-4b0c-98bf-3c338d1b4463> >accessed 24 January 2026

The Cyber Administration of China (CAC) in 2025 released a notice urging the local regulators and social media platforms to adopt “zero tolerance” as an approach to curb the rising doxxing cases. The regulators also stated that the platforms have to –

1. Remove the information that is leaked and take the initiative to shut down the accounts involved
2. Take down the contents related to the sale, methods, or promotion of the practice
3. Launch reporting channels for user complaints.¹⁶

Alongside, in 2020, China introduced Regulations on the Ecological Governance of Online Information Contents to tackle doxxing and other illegal online activities.¹⁷

REMEDIES THAT CAN BE IMPLEMENTED

The Shaviya Sharma case¹⁸ points out that if an individual shares their personal information with a third person, then those details are no longer anonymous. On the other hand, the Supreme Court in the case, District Collector, Hyderabad v. Canara Bank,¹⁹ have stated that an individual’s privacy over their private information cannot be compromised merely because the details are shared with a third party. Both these judgements are contrary to each other, and this stirs confusion and chaos. Therefore, in order to prevent further confusion, it is necessary that India takes up this issue seriously and brings about a new Anti-Doxxing Law with a specific definition as well as proper punishment. Furthermore, the UN Report has emphasised that 1.8 billion, i.e., nearly half of the women and girls in the world, do not have legal protection from digital violence and this flags the need for a proper anti-doxxing law.²⁰

As per the official data, the cybercrimes against women are fewer in number, but the most melancholic fact is that most of these cases go unreported. Most women report these cases anonymously and avoid filing complaints once the obscene image is taken down. Reasons behind this include-

¹⁶Sixth Tone, ‘Zero Tolerance’: China Cracks Down on Doxxing’ <<https://www.sixthtone.com/news/1017157>> accessed 24 January 2026

¹⁷ Supra note.13

¹⁸ Supra note.1

¹⁹ *District Collector, Hyderabad v Canara Bank* 2004 INSC 720

²⁰ UN Women, ‘Digital violence is intensifying, yet nearly half of the world’s women and girls lack legal protection from digital abuse’ (UN Women, 25 November 2025) <<https://www.unwomen.org/en/news-stories/press-release/2025/11/digital-violence-is-intensifying-yet-nearly-half-of-the-worlds-women-and-girls-lack-legal-protection-from-digital-abuse>> accessed 24 January 2026

1. Lack of trust in the justice system and the police
2. Lag in the rendering of justice
3. Harm to the Reputation and public image

Therefore, the authorities have to take up steps to spread awareness so that the targeted victims speak up openly against it and file an FIR so that the wrong doer can be punished and any other person indenting to commit such technology- facilitated gender – based violence (TFGBV) will refrain from doing it.²¹

CONCLUSION

Doxxing is a technology- facilitated gender – based violence (TFGBV) that is rising day by day, and, unfortunately, it is left unrecognised by the legal system. Even though the victims are provided with certain provisions of Bharatiya Nyaya Sanhith,2023 and Information Technology Act,2000, there are no appropriate provisions to apply against it, and this necessitates the need for an apt Anti-Doxxing Law. The upbringing of such a law is meant to protect the constitutional as well as the fundamental rights of the victim.

²¹ Supra note.8