
DOXXING IN INDIA: IS PUBLISHING SOMEONE'S PERSONAL INFORMATION ONLINE A CRIME?

Disha Maheshwari, NMIMS Kirit P. Mehta School of Law

ABSTRACT

The internet has transformed personal information into a readily accessible and highly distributable commodity. Information such as a person's address, telephone number, workplace, photographs and family details can be collected from multiple sources and disseminated to thousands within minutes. This practice, commonly known as “doxxing,” creates a difficult legal question in India because no statute presently recognises doxxing as an independent offence. Instead, harmful disclosures may attract liability under constitutional privacy jurisprudence, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, intermediary regulations and the emerging data-protection framework. This article argues that the principal legal difficulty is not simply whether information is publicly available, but whether its deliberate aggregation and amplification creates a foreseeable risk of serious harm. It proposes a contextual framework based on the nature, source, purpose and consequences of disclosure, while preserving legitimate journalism, whistleblowing and public-interest expression.

Keywords: Doxxing, Privacy, Article 21, Freedom of Speech, Informational Privacy, Cybercrime, Data Protection, Intermediary Liability, Media Law.

I. INTRODUCTION

A person's name may be publicly available. Their professional profile may appear online, their photograph may be on social media, and their address may exist in a public record. Individually, these facts may appear harmless. Yet when they are deliberately collected, combined and broadcast to a large audience, they can become a powerful instrument of harassment or intimidation.

This phenomenon is commonly known as doxxing—the intentional publication or dissemination of personally identifying information, often without consent and in circumstances that may expose an individual to harassment, stalking, intimidation, reputational injury or physical danger.

The problem is particularly significant for media law because publication is not limited to traditional journalists. Digital news organisations, influencers, citizen journalists and ordinary social-media users can all act as publishers. Consequently, regulating doxxing necessarily involves a conflict between two constitutional interests: Article 19(1)(a)'s protection of speech and expression and Article 21's protection of life, liberty and privacy.¹

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Supreme Court recognised privacy as a fundamental right connected with dignity, autonomy and liberty.² At the same time, *R. Rajagopal v. State of Tamil Nadu* recognised the relationship between privacy and freedom of the press, including the significance of information contained in public records.³

This article argues that India does not presently criminalise doxxing as a standalone offence. Instead, different forms of harmful disclosure are addressed through a fragmented legal framework. More importantly, the law should move beyond the simplistic distinction between “public” and “private” information and recognise the difference between availability, aggregation and harmful amplification.

II. THE CONSTITUTIONAL TENSION: PRIVACY VERSUS EXPRESSION

The constitutional foundation for regulating doxxing lies in the right to privacy. In

¹ INDIA CONST. art. 19(1)(a), INDIA CONST. art. 21.

² *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, 135–37 (India).

³ *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632, 639–51 (India).

Puttaswamy, a nine-judge Bench unanimously recognised privacy as a fundamental right under the Constitution. The judgment recognised informational privacy as an important dimension of individual autonomy, emphasising that individuals have an interest in controlling information concerning themselves.⁴

This principle is directly relevant to doxxing. Personal information can reveal an individual's relationships, movements, family, financial affairs and physical location. Its uncontrolled dissemination may therefore interfere with autonomy and dignity even where individual pieces of information are not inherently secret.

However, privacy is not absolute. Article 19(1)(a) protects freedom of speech and expression, and legitimate journalism frequently requires publication of information concerning individuals.

This balance was considered in *R. Rajagopal v. State of Tamil Nadu*. The Supreme Court recognised an individual's right to privacy but also held that matters forming part of public records could generally be published and commented upon.⁵ The Court nevertheless distinguished private matters from matters connected with the discharge of public functions.⁶ The principle is crucial in the digital context. Publishing a report that a public official is being investigated for corruption is materially different from publishing the official's home address, private telephone number and children's school details.

The first may contribute to public accountability. The second may contribute little to public understanding while increasing the risk of harassment. Thus, public interest should not be confused with public curiosity.

III. DOES THE INFORMATION TECHNOLOGY ACT CRIMINALISE DOXXING?

The answer is no, not as a general offence.

The Information Technology Act, 2000 contains provisions capable of addressing particular forms of harmful disclosure, but none creates a comprehensive offence of doxxing.

⁴ *K.S. Puttaswamy*, (2017) 10 SCC, at 135–37 and at 147–50.

⁵ *R. Rajagopal*, (1994) 6 SCC at 650–51.

⁶ *R. Rajagopal*, (1994) 6 SCC at 651.

A. Section 66E

Section 66E criminalises the intentional or knowing capture, publication or transmission of an image of a person's private area without consent in circumstances violating privacy.⁷ This provision may apply where an intimate image is disseminated without consent. However, it does not automatically apply when a person's residential address, telephone number or workplace is published. This distinction demonstrates the fragmented nature of Indian cyber law.

B. Sections 72 and 72A

The Act also addresses breach of confidentiality and privacy and disclosure of information in breach of a lawful contract. Section 72A may be relevant where personal information has been obtained in the course of a contractual relationship and subsequently disclosed improperly.⁸

Yet these provisions remain fact-specific. A person who maliciously publishes another person's address obtained from publicly accessible material may not fall neatly within them. Consequently, Indian law regulates particular consequences of disclosure, rather than doxxing itself.

IV. WHEN DOXXING BECOMES A CRIMINAL OFFENCE

Although doxxing is not a standalone offence, the conduct surrounding it may attract criminal liability. For example, Section 351 of the Bharatiya Nyaya Sanhita, 2023 criminalises criminal intimidation, including threats concerning a person's person, reputation or property where the statutory requirements are satisfied.⁹

Therefore, if an individual publishes someone's residential address while threatening to send people to their home, the conduct may potentially constitute criminal intimidation. The offence, however, arises from the legally defined threatening conduct—not merely from publication of the address.

Similarly, Section 356 of the BNS deals with defamation. If personal information is published alongside false imputations intended or likely to harm reputation, defamation may become

⁷ Information Technology Act, No. 21 of 2000, § 66E, India Code (2000).

⁸ Information Technology Act, No. 21 of 2000, § 66E, India Code (2000).

⁹ Bharatiya Nyaya Sanhita, No. 45 of 2023, § 351 (India 2023).

relevant.¹⁰

This distinction is important: publishing personal information is not automatically defamation, just as it is not automatically criminal intimidation. Liability depends on the statutory elements and surrounding circumstances.

V. INTERMEDIARY LIABILITY AND SOCIAL MEDIA

Doxxing becomes more complicated when information is distributed through social-media platforms.

Section 79 of the Information Technology Act provides qualified safe harbour to intermediaries for third-party information, subject to statutory conditions.¹¹ In *Shreya Singhal v. Union of India*, the Supreme Court considered the constitutionality of this framework and read down the “actual knowledge” requirement, emphasising the importance of court orders or appropriate government action in triggering intermediary obligations.¹² This approach protects against a system in which platforms would be required to remove content merely because an individual alleges that it is unlawful. At the same time, victims of doxxing may face immediate risks while waiting for formal proceedings.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 therefore require intermediaries to undertake reasonable efforts concerning specified categories of unlawful or privacy-invasive content and provide grievance mechanisms. The Rules also contain an expedited mechanism concerning certain intimate or privacy-invasive material.¹³

The challenge is therefore to create a system that is fast enough to protect victims but sufficiently constrained to avoid private censorship.

VI. THE DPDP ACT AND THE PROBLEM OF PUBLICLY AVAILABLE INFORMATION

The Digital Personal Data Protection Act, 2023 adds a new dimension to this debate. Its objective is to regulate the processing of digital personal data while protecting individual’s

¹⁰ Bharatiya Nyaya Sanhita, No. 45 of 2023, § 351 (India 2023).

¹¹ Information Technology Act, No. 21 of 2000, § 66E, India Code (2000).

¹² *Shreya Singhal v. Union of India*, (2015) 5 SCC 1, 92–97 (India).

¹³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(b).

interests in their personal data.¹⁴

However, the Act should not be described as an anti-doxxing statute. Its regulatory framework primarily concerns the processing of digital personal data by entities within its scope, and its provisions have been brought into force in phases. The Digital Personal Data Protection Rules, 2025 likewise provide for staggered commencement of different provisions.¹⁵

The more interesting issue is the relationship between data that is publicly available and data that is legitimately reusable. Suppose a person's name, workplace and photograph are separately available online. Another individual then combines them with a residential address, family information and telephone number and broadcasts the compilation to thousands of followers. The harm may not arise from any single data point. It may arise from aggregation. This suggests that privacy law must recognise that information can become significantly more intrusive when different pieces are assembled into a single profile.

Therefore: Publicly accessible information should not automatically be treated as information whose unrestricted aggregation and amplification is always justified.

VII. FROM PRIVACY TO AMPLIFICATION: THE LEGAL GAP

The central weakness of the present framework is its tendency to examine individual pieces of information rather than the effect produced by their combination.

A useful framework for determining whether a disclosure should attract legal scrutiny would consider four factors.

1. Nature of the information

Is it professional information, a public record, a residential address, financial information, information concerning children or intimate material?

2. Source

Was the information voluntarily disclosed, obtained from a public record, legitimately

¹⁴ Digital Personal Data Protection Act, No. 22 of 2023, pmbl. (India 2023).

¹⁵ Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025).

investigated, leaked or obtained through unauthorised access?

3. Purpose

Was the purpose journalism, whistleblowing, public accountability or public safety? Or was it harassment, retaliation, intimidation or revenge?

4. Foreseeable harm

Was the disclosure reasonably capable of facilitating stalking, threats, physical violence, fraud, harassment or serious reputational harm?

This may be called a Context–Purpose–Harm framework.

It avoids two equally problematic extremes: treating every disclosure as unlawful or treating every publicly available fact as permanently free from privacy concerns.

VIII. SHOULD INDIA CREATE A STANDALONE ANTI-DOXXING OFFENCE?

There is a legitimate argument for legislative reform because victims currently have to navigate several different legal provisions depending on the nature of the conduct.

However, a broadly worded offence criminalising the “publication of personal information without consent” could seriously affect legitimate journalism and public-interest expression.

Investigative reporting may require identifying individuals. Whistleblowers may need to disclose information. Public officials may legitimately be subjected to scrutiny.

Therefore, any future anti-doxxing provision should focus on harmful and unjustified disclosure, rather than disclosure alone.

The law could define doxxing around intentional dissemination or aggregation of identifying information where there is no legitimate justification and where serious harm is reasonably foreseeable.

A statutory public-interest defence should protect journalism, whistleblowing, court reporting, democratic accountability and disclosures necessary to prevent serious wrongdoing.

IX. RECOMMENDATIONS

First, India should develop a clear statutory definition of harmful doxxing.

Second, legislation should expressly distinguish public availability from public interest. The mere existence of information online should not conclusively determine whether its mass republication is justified.

Third, victims should have access to a rapid and transparent mechanism for removing information such as residential addresses, private telephone numbers, intimate images and information concerning children where disclosure creates a substantial risk of harm.

Fourth, intermediary regulation should distinguish between the original publication of information and its subsequent deliberate amplification. Platforms that receive credible complaints concerning serious privacy threats should have clearly defined and time-bound procedures for review and removal.

Finally, any reform must preserve constitutional safeguards for journalism and legitimate expression.

X. CONCLUSION

Is publishing someone's personal information online a crime in India?

Not automatically.

India does not presently recognise “doxxing” as a single, standalone criminal offence. Nevertheless, particular forms of disclosure may attract consequences under privacy jurisprudence, the Information Technology Act, the Bharatiya Nyaya Sanhita, intermediary regulation and data-protection law.

The deeper problem is therefore not simply the absence of a criminal provision. It is the difficulty of applying traditional concepts of privacy to a digital environment where information can be collected, combined and amplified within seconds.

The law should consequently move beyond asking only:

“Was this information publicly available?” It should also ask:

“Why was it disclosed, why was it amplified, and was serious harm a reasonably foreseeable consequence?”

The objective of future regulation should not be to suppress uncomfortable information or weaken the press. It should be to prevent the transformation of personal information into an instrument of intimidation while preserving legitimate public-interest expression.

In the digital age, privacy is therefore not simply about keeping information secret. It is increasingly about who controls its context, scale and consequences.