

Unveiling Doxing: The Impact and Legal Landscape in India

Vallimireddy Abhinav Deep Dora^{1*}, Surla Sireesha², L. Haritha³, D. Chanikya Chandra Sekhar⁴, Mohamad Mokdad⁵

^{1,2,3}Vignan Institute of Law, Vignan Foundation for Science, Technology and Research, Guntur, Andhra Pradesh, India.

⁴Department of Law, A.P. High Court, Amaravati, Andhra Pradesh, India.

⁵Department of Public Policies, Zaragoza University, Zaragoza, Aragón, Spain.
abhinavvallimireddy@gmail.com¹, sireesha4197@gmail.com², haritha.lanke@gmail.com³,
chanikyachandrasekhar@gmail.com⁴, mhdmdk@gmail.com⁵

Abstract: Even in this AI era, where personal apps rule the internet and privacy is prioritized by the courts, there are still countless cases where people's personal information is stolen and made public. "Doxing" is "throwing out dox," where "dox" is a synonym for papers. The practice of disclosing personal and identifiable data regarding individuals online is known as "doxing," or "doxing." Due to the vast diversity of search methods and the ease of access to online data, anyone can become a victim of doxing. If you have ever commented on an online forum, used a social networking site, signed an online petition, or bought a house through real estate, purchased goods online, your information is accessible to the public. Searching public databases, local records, government documents, search engines, and other archives yields a wealth of information. The Indian Act neither defines nor criminalizes doxing. However, doxing falls under various legal categories. It is covered by S. 354C & 354D of the IPC, 1860, S. 67 of the IT Act, and other provisions, depending on the offence. This study will critically evaluate India's anti-doxing mechanism and the legislative frameworks of other countries. Finally, it discusses how India should combat this social issue.

Keywords: Data Protection and IT Law; Doxing and Privacy; Digital Wellbeing; Global Cybercrime Calls; Personally Identifiable Information and IT Act; Universal Declaration of Human Rights; International Covenant on Civil and Political Rights.

Received on: 14/06/2025, **Revised on:** 21/08/2025, **Accepted on:** 18/10/2025, **Published on:** 05/06/2026

Journal Homepage: <https://www.fmdbpublish.com/user/journals/details/FTSPL>

DOI: <https://doi.org/10.69888/FTSPL.2026.000679>

Cite as: V. A. D. Dora, S. Sireesha, L. Haritha, D. C. C. Sekhar, and M. Mokdad, "Unveiling Doxing: The Impact and Legal Landscape in India," *FMDB Transactions on Sustainable Public and Law*, vol. 1, no. 2, pp. 60–70, 2026.

Copyright © 2026 V. A. D. Dora *et al.*, licensed to Fernando Martins De Bulhão (FMDB) Publishing Company. This is an open access article distributed under [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/), which permits copying, remixing, redistributing, transformation, and building upon the material in any medium so long as the original work is properly cited.

1. Introduction

Doxing is typically a malicious act committed against an individual by a hacker or another person for a specific purpose, such as to humiliate or harm the person. Usually, the intent is to humiliate or degrade the victim [1]. For instance, to discredit a private message board troll, hackers may divulge their name. The released data includes potentially dangerous and harmful information. Their goals can be anything from monetary gain to personal revenge [2]. In December 2011, when hacktivists released detailed data on about 7,000 law enforcement personnel in their reaction to investigations into hacking operations,

*Corresponding author.

doxing became well-known [3]. This instance highlighted the possible negative effects of doxing, which can range from less serious outcomes like undesired deliveries to more serious ones like bullying or physical abuse [4]. Celebrities, politicians, and entrepreneurs are just a few of the prominent figures who have been harmed by this intrusive action, putting their lives and safety at risk. Whatever the justification, doxing is an obvious invasion of privacy that has serious consequences for those who are targeted [5]. Doxing is a severe danger to one's privacy and personal safety that can have a large impact on people as well as their communities. Its effects are not limited to the digital sphere; they frequently lead to harassment, stalking, and even physical assault in real life [6]. Doxing is becoming more common in India, where internet connectivity is rising quickly. Doxing is the malicious act of publicly revealing an individual's personal information. Information such as residential address, mobile number, personal photos and videos, etc., This doxing is happening in many social media platforms and getting consolidated with other offences such as defamation, insulting the modesty of women, criminal intimidation by anonymous communication [7].

In India, the act of doxing can lead to serious consequences, including harassment, stalking, intimidation, damage to one's reputation, emotional distress, and even physical danger [8]. Those who fall victim to doxing frequently endure continuous harassment, online trolling, particularly when their personal information is exposed to a wide online social media platform [9]. This issue is especially severe for women, celebrities, and public figures, who are often singled out because of their political beliefs, gender, or views [10]. The online anonymity offered by these platforms makes it easier for offenders to commit these acts without facing immediate punishment [33]. At the same time, the victims often struggle to find legal action or protection. Under Indian law, doxing falls within the broader ambit of cybercrimes and privacy violations, even though it is not specifically addressed by law [11]. There are some doxing-related offenses under the IT Act 2000 and the Bhartiya Nyaya Sanhita 2023, such as stalking, defamation, criminal intimidation by anonymous communication, identity theft, publishing obscene material, and breaches of confidentiality and privacy [12]. Doxing includes revealing a wide range of personal information about victims, such as names, addresses, phone numbers, and more, with the intention of harming their reputation [13]. Victims may face unintentional publication of personal information online, leading to violations of state or federal laws. Anti-doxing legislation has been enacted in many jurisdictions to prevent such violations, as seen in cases like the mistaken identity of an Arkansas professor during a Neo-Nazi demonstration [14].

1.1. Objective

To facilitate discussions on the legal strategies needed to address doxing effectively. The research findings revealed that there is no recognized definition of "doxing" within Indian Criminal Laws, Privacy Laws, human rights law in general, or international law in particular [15].

2. Literature Review

Khushi et al. [35] shed light on the increase in doxing incidents during the COVID-19 crisis, especially aimed at women and those on the fringes of society [16]. They point out that the move towards online communication made people more susceptible to attacks, as it provided cover for those who wanted to harass others [17]. The emotional toll of being doxed can be significant, causing victims to suffer from stress and distress [32]. The researchers advocate for better laws and rules for online platforms to tackle and stop doxing, highlighting the critical need for thorough support networks for those affected by digital violence based on gender [18]. Mohanty [2] provides a broad analysis of cybercrimes, including doxing, which pose a significant global threat to individuals and businesses alike [19]. Doxing, the malicious act of publicly revealing personal information, often leads to harassment and emotional distress for victims [20]. In a digital landscape rife with identity theft, sextortion, and ransomware, perpetrators exploit vulnerabilities for financial gain [21]. The rise of doxing reflects the urgent need for enhanced cybersecurity measures and legal frameworks. Collaborative efforts among governments, corporations, and law enforcement are essential to combat these crimes and protect individuals from the severe repercussions of cyber harassment and abuse [22].

2.1. Types of Doxing

Doxing can take many forms, including swatting, doxing, revenge doxing, faulty doxing, and celebrity doxing, each with different motivations and consequences [23]. Doxing can lead to serious consequences, like suicide, degradation of reputation, loss of job, physical and mental harassment, etc. Laws in India address cyber harassment, stalking, voyeurism, defamation, and online stalking, with penalties for offenders [24]:

- **Celebrity Doxing:** The public disclosure of private details about well-known people, often motivated by curiosity, admiration, or vengeance. This can lead to threats, physical follow-ups, and identity theft.
- **Incorrect Doxing:** The public release of inaccurate or misleading data about an individual, often due to negligence or inadequate investigation. This results in threats and damage to one's reputation.

- **Retaliatory Doxing:** The public sharing of personal information as a means of revenge, typically following personal conflicts. This can lead to intense threats, defamation, and issues with mental well-being.
- **Armed Police Response Doxing:** The public sharing of personal details to provoke a police reaction, often for amusement or to intimidate. This can result in injuries, fatalities, and legal issues.
- **Intimidation Doxing:** The public release of personal information about politicians, activists, or those with differing opinions to scare or silence them. This can lead to targeted threats and violence.
- **Business Doxing:** The public sharing of personal details about business leaders or companies to harm their reputations or interfere with their operations. This can lead to financial and reputational harm.
- **Community Doxing:** Online groups exposing personal details to either punish or discredit individuals. This can lead to organized threats and long-term effects.

The effects of doxing include damage to one's reputation, loss of job opportunities, threats, physical violence, legal penalties, and psychological distress [34]. In India, various legal frameworks under the IPC and IT Act can be used to address doxing cases [35].

2.2. IPC (Indian Penal Code)

In IPC, it does not specifically mention doxing, but various provisions are invoked to explain the concepts of doxing and malicious intent. Some provisions show the impact, such as doxing under IPC S. 354C, 354D, and 499. According to S. 354C, any man who captures the image of any woman engaging in a private act without her consent commits the crime of voyeurism. Voyeurism becomes doxing in cases where voyeuristic content, such as images or videos, is obtained and shared online without consent. Doxing violates both S. 354C and other privacy laws in India [25]. As per S. 354D, any man who monitors the actions of women on the internet or any other electronic communication, repeatedly follows through any means, including the internet, shall be punishable. It is considered cyberstalking, which is applicable as doxing, where stalking any individual's online presence to extract the personal details or continuously observing actions for not a personal gain or financial benefit but to cause shame or emotional harm to the victim in public. Both doxing and stalking are closely related crimes where published personal information gives access to a stalker to follow and harm the victim. Doxing helps expose the victim's information, which is essential for stalkers to monitor. Even though doxing is not clearly mentioned in any provisions, it is impacting individuals in society [26]. The absence of specific laws against doxing creates a legal challenge for victims. In S. 354C and 354D, it focuses on the women victims, but doxing could affect men and non-binary individuals, so there is a need for gender-neutral laws that protect individuals equally [27].

Doxing and defamation are intertwined by the harm they cause to one's reputation. Doxing is the act of revealing personal details without permission, which can lead to embarrassment in public, isolation from society, or damage to one's career, all of which are considered defamation. This can occur on social media, online discussion boards, or for revenge. These situations involve a deliberate intent to cause harm, the disclosure of private information, and damage to one's reputation, all of which qualify as defamation under S. 499 of the IPC [28]. Individuals who have been victims of doxing in India may pursue legal action under the Defamation Act (S. 499 of the IPC) and the IT Act, 2000. Criminal defamation (S. 499 of the IPC) permits victims to seek redress for damage to their reputation, which may result in penalties under S. 500 of the IPC. Section 66E of the IT Act addresses unauthorized sharing of private photos or information. Civil defamation allows victims to seek financial compensation. Section 354D of the IPC criminalizes cyberstalking, which is relevant to cases of doxing that result in harassment or stalking. The connection between doxing and defamation is evident, as doxing frequently leads to damage to one's reputation [29]. The intent to cause harm in doxing is closely related to defamation, and victims can seek legal action under both defamation laws and the IT Act. As technology advances, legal systems must evolve to safeguard individuals from the negative effects of doxing and defamation, which requires increased public awareness, stronger enforcement, and updates to legal policies [30].

2.3. IT Act, 2000

In India, the IT Act, 2000, addresses cybercrimes such as doxing under S. 66C, 66E, 67, and 72, focusing on privacy breaches and the dissemination of harmful content. S. 66E deals with privacy violations, penalizing the unauthorized sharing of private images. It is relevant in cases of doxing involving sensitive or explicit images. S. 66C of the IT Act, 2000 deals with Identity theft. Anyone who fraudulently or dishonestly uses another person's electronic signature, password, or other unique identification feature can be imprisoned for up to three years and fined up to one lakh rupees [31]. Doxing refers to distinct yet interconnected methods of exploiting personal information, each with its own objectives and methodologies. Identity theft encompasses the unauthorized acquisition of an individual's personal data, including but not limited to their name, Social Security number, or credit card information, to assume their identity for financial gain, perpetrating fraud, or engaging in other illicit activities. The central objective of identity theft is to commit fraudulent acts, mislead others, and derive advantages from the victim's identity, frequently resulting in significant financial and legal repercussions for the victim.

Conversely, doxing, also known as “doxing,” pertains to the dissemination of an individual’s private or personally identifiable information (PII) to the public without their consent. This may include home addresses, phone numbers, or social media profiles. The primary motivation behind doxing is typically to harass, threaten, or intimidate the victim by making their private information accessible to a wider audience, potentially leading to real-world consequences such as stalking or physical threats. While financial motives often drive identity theft, doxing is more commonly linked to personal vendettas, acts of revenge, or tactics aimed at intimidation. S. 66E of the IT Act, 2000 deals with breaches of personal privacy, especially concerning the unauthorized capture, sharing, or distribution of private photographs. It makes it a crime to intentionally capture or share an image of someone’s private areas without their permission, especially when that person has a legitimate expectation of privacy. This S. imposes a penalty of up to 3 years’ imprisonment, a fine of up to Rs. 2 lakhs, or both. When it comes to doxing, S. 66E becomes particularly significant when the act involves sharing sensitive or explicit photos of an individual. For instance, revenge doxing often includes the unauthorized release of private, intimate photos or videos of a victim.

These photos are typically taken in a private setting and shared either during or after a relationship has ended. The motive is often to humiliate or seek revenge against the victim, and the spread of such content can cause considerable psychological and reputational damage. If a person posts private or intimate photos of another person online as part of a doxing attack, S. 66E can be used to hold the perpetrator responsible for violating the victim’s privacy. The law would hold the perpetrator accountable for sharing private information obtained without consent and distributed with the intent to cause harm. S. 66E serves to protect individuals from having their most private moments shared with the public, especially in scenarios where the disclosure of such information can lead to harassment or harm. Doxing incidents involving personal images or videos that infringe on someone’s privacy can thus be prosecuted under S. 67 of the IT Act, 2000, which addresses the distribution of offensive content online. This S. makes it illegal to distribute any content that is “offensive or arouses sexual desire” and is expected to corrupt or degrade the mental state of its audience. Individuals found guilty under S. 67 may be sentenced to up to 5 years in jail and fined up to Rs. 10 lakhs for their first offense, with increased penalties for subsequent offenses. Concerning the act of doxing, S. 67 is particularly relevant in instances where the doxer shares or spreads offensive or sexually explicit content without the victim’s permission.

This could include the unauthorized distribution of pornographic content or the dissemination of explicit images of a victim. The motive behind such doxing is typically to inflict embarrassment, shame, or psychological distress on the victim, leading to significant personal, professional, and social repercussions. In cases involving revenge porn, where private videos or images of a person are uploaded to the internet without their consent, S. 67 can be applied. This provision would encompass scenarios in which an individual uploads offensive content with the aim of defaming, shaming, or harassing the victim. S. 67 expands the protection against doxing by concentrating on the nature of the content, ensuring that those who distribute offensive or sexually explicit content are held accountable. By establishing legal repercussions for such actions, S. 67 acts as a deterrent for doxers who wish to harm others by exposing explicit or sexual content online. S. 67 of the IT Act, 2000, criminalizes the transmission of obscene material, applicable when doxers release sexually explicit content without consent. This S. aims to prevent harm and humiliation caused by the dissemination of such material. S. 72 addresses the breach of confidentiality and privacy, punishing unauthorized access to personal information shared without consent. It is relevant in cases where doxers obtain and disclose private data unlawfully. The link between doxing and these provisions of the IT Act, 2000 lies in their collective approach to addressing privacy violations, the dissemination of obscene content, and breaches of confidentiality.

While doxing is not explicitly mentioned in the Act, S.S 66C, 66E, 67, and 72 offer legal remedies for victims. These S.S provide a framework for addressing different aspects of doxing, ensuring that perpetrators face consequences for their actions. Doxing is a growing concern in India, with personal information leaked online leading to harassment and harm. The IT Act, 2000, through S.S 66C, 66E, 67, and 72, provides legal recourse for victims of doxing by addressing privacy violations, the dissemination of obscene content, and unauthorized access to personal information. The evolving legal landscape in India aims to protect individuals from cybercrimes such as doxing, ensuring their rights to privacy and dignity in the digital age. In *Puttaswamy vs Union of India* [10], the Supreme Court of India ruled that the right to privacy is protected as an inherent part of the right to life and personal liberty under Article 21 and as one of the freedoms guaranteed by Part III of the Constitution. This declaration arose from a series of writ petitions challenging the constitutional validity of the UID (Aadhaar) paper and the central government’s January 2009 notification establishing the Unique Identification Authority of India (UIDAI). The Privacy Judgment recognized nine different modes of privacy, including communicational privacy & informational privacy. The right to privacy was emphasized as an essential facet of human dignity.

The Aadhaar Act was passed as a Money Bill by the Lok Sabha, bypassing the Rajya Sabha’s reservations. The Act mandated linking Aadhaar to various services and benefits, as well as the collection of children’s biometric data. The Supreme Court’s 2018 Aadhaar judgment upheld the Act’s validity, despite concerns about privacy violations and the government’s disobedience of interim orders. The dissenting judge highlighted the potential impact on citizens’ lives and the overbroad nature of the requirements. The Privacy Judgment has been invoked in various cases to protect decisional privacy and to challenge laws that infringe on privacy rights. However, the judiciary’s response to privacy enforcement efforts has not always been encouraging.

Instances of data theft, leaks, and surveillance highlight the challenges posed by digital technology. The increasing reliance on Aadhaar for various transactions and services has raised concerns about exclusion and privacy violations. The lack of a comprehensive data protection law further exacerbates these issues. The judgment in the Puttaswamy case emphasized the importance of safeguarding individuals against unauthorized encroachment into their private affairs, including the wrongful exploitation of personal information.

Doxing violations of this right entail the disclosure of confidential data, including addresses, telephone numbers, and other identifying information, often resulting in harassment, threats, or physical harm. In the case of Singh [11], the plaintiff, Shaviya Sharma, has filed a suit against Squint Neon and others, alleging that they engaged in “doxing” by searching for and circulating private information about her. The plaintiff posted a tweet about a public political figure, prompting multiple tweets and posts on various Twitter handles. These tweets disclosed her professional identity, photographs, and an email written to her employer. The plaintiff requested an injunction prohibiting others from misusing her photographs and identity for any purpose without her consent. The court noted that “It’s clear that allowing Doxing to continue without control could lead to breach of privacy rights. It’s noted that the term ‘Doxing’ is not clearly defined in Indian law and has not been made a criminal offense in the country. The concept of “doxing” is derived from releasing personal documents or information about someone, a practice that began in the 1990s to expose individuals who valued anonymity. It’s also pointed out that even if Doxing isn’t used for sexual harassment, the exposure of personal data online can still be imperiled due to the public disclosure of private, sensitive, and personal details.

The widespread availability of the internet, along with the ease of access to technology, has made a person’s online and offline lives intertwined. As a result, actions taken online can have significant offline consequences for the individual involved. The court also mentioned that “The internet provides a broad audience, thereby increasing the likelihood of violence occurring in response to Doxing. When someone’s personal information is made public for the world to see, especially in serious situations, threats and violent responses can come from anywhere. Doxing poses a greater risk to physical safety compared to other forms of cyberbullying and harassment, as the potential for real-life harm increases with access to personal details like a person’s residence. However, it’s also noted that if information is publicly available or accessible, there’s no legal issue. Therefore, the court must find a careful balance between allowing access to public information and protecting individual privacy”. The future implications of AI and other technologies for privacy and human autonomy are a growing concern. The rise of digital surveillance, data manipulation, and AI-driven decision-making poses threats to individual rights and freedoms. The need to balance technological advancements with privacy protection is crucial in ensuring a secure and empathetic society.

3. International Overview on Doxing

On the legal frameworks within certain jurisdictions, all of which have implemented measures to safeguard individuals from doxing, a form of online harassment. Examination of laws in England, the United States, the European Union, and International human rights law was undertaken. The research scope extended to explore current laws regulating doxing, as well as potential legal areas such as copyright, defamation, and consumer protection. The right to privacy, enshrined in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), is pertinent in today’s digital world. Doxing, which exposes private information, infringes on this right, often leading to threats and harm, thereby violating the right to security and protection from harm. While Article 19 of ICCPR itself declares freedom of expression is a fundamental right, doxing can be an abuse of this right when it results in harm to others.

Doxing disproportionately affects marginalized groups, perpetuating discrimination and inequality, and infringing on the right to equality and non-discrimination. Women, racial minorities, LGBTQ+ individuals, activists, and journalists are often targeted, leading to significant implications for women’s rights and the right to participate in public life. Doxing undermines the work of human rights defenders, activists, and journalists, exposing them to personal and professional risks and violating the right to freedom of the press. Although doxing is not explicitly mentioned in international human rights treaties, it is connected to several fundamental rights, including the right to privacy, the right to security, freedom of expression, and protection from discrimination. Ensuring robust legal protections against doxing and holding perpetrators accountable is essential to upholding these rights.

3.1. European Union

The European Union lacks a dedicated law on doxing. Yet, it could be interpreted under the General Data Protection Regulation (GDPR) and a proposed Directive on combating violence against women and domestic violence. In New Zealand, the offense is likely to fall under the Harmful Digital Communications Act. Doxing, or the act of publicly revealing someone’s personal information without their consent, is not clearly defined by EU laws. However, various regulations and legal frameworks do address its consequences, particularly in areas such as data protection, cyber violence, and the dissemination of illegal online content. The “General Data Protection Regulation (GDPR)” grants individuals the ability to manage their personal information,

including the rights to access, amend, and delete it, which can be relevant in instances of doxing. Although the GDPR applies when personal information is shared unlawfully, its scope is limited, as it does not cover purely private or domestic activities involving manual data processing.

In 2021, the European Parliament recognized doxing as a type of “cyber violence”, particularly affecting women and girls, leading to a March 2022 proposal for a “Directive on combating violence against women and domestic violence”. This proposal includes “Article 8”, which criminalizes the unauthorized publication of someone’s personal information with the intent to cause harm, and “Article 9”, which targets the encouragement of violence through threatening or insulting content. The “Digital Services Act (DSA)” also requires online platforms to remove illegal content, including doxing, in member states where it is illegal under national law. For instance, France has made doxing illegal under Article 223-1 of its Criminal Code, which carries penalties of up to “EUR 45,000” and “three years imprisonment” for the unauthorized sharing of personal information with the intent to cause harm. Likewise, “Germany” permits victims to seek legal injunctions under its civil law and uses the GDPR to enforce privacy violations. Therefore, while doxing is not explicitly defined by EU laws, a combination of EU-wide data protection regulations, proposed directives, and national laws in countries like France and Germany provides a framework to address and combat doxing effectively.

3.2. United States of America

There is no legally binding federal definition of doxing in the United States. However, some state laws address the concept. In California, the general concept of doxing is covered by California Penal Code S. 653.2. This section makes it illegal to share personally identifiable information or digital images with the intent to cause a third party to engage in physical contact, harm, or harassment. A conviction under this law is a misdemeanor, with a maximum jail sentence of one year. Additionally, a fine of up to \$1,000 may be imposed. Another law, California Government Code S. 6218.01, protects the personal information of people working in healthcare settings, including abortion clinic staff. This law prohibits the posting of personal information or images of healthcare workers, patients, or others. It increases penalties for violations to include imprisonment for up to 1 year, a fine of up to \$10,000, or both, with penalties escalating to \$50,000 for violations that result in bodily harm. In Texas, a new offense called “The Unlawful Disclosure of Residence Address or Telephone Number,” S. 42.07452 of the Texas Penal Code, which includes doxing, was introduced. This law went into effect in 2023, intending to target internet posts that reveal a person's home address or phone number with the intent to cause or threaten harm to the individual or a member of their family or household.

A person commits this offense if they post an individual's residence address or phone number on a publicly accessible website with the intent to cause or threaten harm to the individual or a member of their family or household. Depending on the circumstances, the crime could be classified as a Class B or Class A misdemeanor. If the violation causes bodily harm to the doxing victim or any member of the victim's family or household, a Class A misdemeanor is charged. Otherwise, it is a class B misdemeanor. Regarding doxing, individuals who believe they have been doxed on social media should initially hope that the platform considers the content a violation of its community guidelines. If the platform does not consider the content to violate these guidelines, it will remain available for others to view. Then, even when a user blatantly breaks a website's rules, as per S. 230 of the Communications Decency Act, it prevents that user from filing a lawsuit against the social media platform if it doesn't properly enforce its doxing policy. S. 230 also completely shields social media platforms from being held civilly responsible. As a result, victims of doxing on social media platforms cannot legally hold the platform accountable for enabling the doxing. *Barnes v. Yahoo!, Inc.* serves as a clear illustration of how these realities of social media can harm victims.

In this case, the victim's ex-boyfriend fabricated a Yahoo! public profile for her and uploaded nude photos taken without her consent. He also included her personal and work contact information on the profile. The ex-boyfriend then used the fake profile to attempt to engage in sexual conversations with others on the site's chatroom. Following numerous unsolicited phone calls, emails, and personal visits from strangers, the victim tried Yahoo!'s own methods to request the removal of the fake profile. These efforts were unsuccessful, leading the victim to file a lawsuit against Yahoo! for its negligent failure to remove the unauthorized profile. The court ruled in favour of Yahoo!, citing S. 230 as a defense against liability. If this kind of legal issue arises in India, the situation could be examined as per S. 79 of the IT Act, 2000, which provides intermediary liability protections akin to those in “S. 230 of the U.S. Communications Decency Act (CDA)”. This S. states that intermediaries, like Yahoo!, are not responsible for content posted by others, so long as they meet specific obligations, including promptly removing illegal content upon being notified.

If the person reporting the content to the platform does not receive a response within the specified time, the platform could lose its immunity and face legal consequences. Moreover, under the “Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021”, platforms are required to delete offensive or unauthorized content, including personal details shared without consent or explicit images, within 24 hours of receiving a complaint. If a social media platform does not adhere to these guidelines in an Indian situation, the complainant could take legal action against the platform for failing to comply.

Regarding legal action, individuals affected by doxing in India can seek redress under various S.s of the Bhartiya Nyaya Sanhitha 2023, such as S. 78 (stalking), S. 356 (defamation), or even under the Indecent Representation of Women (Prohibition) Act. Also, the IT Act, through S.S 66E and 67, penalizes the unauthorized sharing of personal or explicit images, providing additional grounds for legal proceedings.

3.3. England

In England, there is also no specific definition for doxing. Still, victims of doxing have multiple avenues for redress or legal action, including the Protection from Harassment Act (PHA) 1997, the Online Safety Act 2023, and the Malicious Communications Act (MCA) 1988:

- The Online Safety Act 2023 aims to regulate the UK's digital landscape. This Act includes provisions for content moderation, putting more pressure on technology and social media companies to remove specific content from their platforms under certain conditions. Initially, the Bill proposed adult safety responsibilities that would criminalize 'legal but harmful' content on appropriate platforms. However, these S.S were removed from the final version and replaced with duties centered on transparency, accountability, and freedom of expression.
- Legal content platforms must address specific types of content and empower users, as outlined in these duties. Certain online platforms must also establish clear terms of service regarding the restriction or removal of content that violates these terms. Doxing could be covered by the Act's provisions requiring platforms to moderate and remove content related to criminal activity. However, the scope of these provisions is limited to the removal of doxing content and does not necessarily criminalize the act or require compensation for the victims.

It may be illegal under other criminal statutes. For example, the Protection from Harassment Act (PHA) 1997 establishes two primary harassment offences: harassment under Section 2 and harassment causing fear or violence under Section 4. To be considered harassment, doxing must be part of a 'course of conduct' that includes multiple instances. Seeking a conviction for this offense is limited to cases involving multiple related actions and may not apply to a single instance of doxing. Doxing could also be considered a stalking offense under the same Act. Stalking, like harassment, must be part of a pattern of behavior and involve multiple instances of related actions. If a doxing incident involves publishing a statement or other material about a person or monitoring their internet, email, or other electronic communication, it may constitute stalking. If the actions preceding the offense occur online, they may constitute cyberstalking. There is currently no specific legal definition or laws governing cyberstalking, and the Crown Prosecution Service's Stalking and Harassment Guidance clarifies that the specific circumstances of each case determine whether an action is lawful.

Sending inappropriate or offensive messages, known as doxing, may be considered illegal under the Malicious Communications Act (MCA) of 1988. This act defines malicious communication as any written or verbal message that is indecent, grossly offensive, threatening, or contains false or believed-to-be false information, and is sent to another person with the intent to cause distress or anxiety. The Social Media Guidelines also state that the specifics of the case determine whether a message posted on social media is legal, as it must be addressed to a specific individual. Sending an electronic notification with the intention of causing distress or anxiety may also be classified as an offensive or threatening message under the Communications Act 2003. The legal definition is more limited than under the Malicious Communications Act, as S. 127 of the Communications Act 2003 only applies to communications sent over a public network that are deemed grossly offensive, indecent, or obscene. It is not necessary to demonstrate that the message was received by the intended recipient, which includes posting it on a website. Doxing may also be grounds for a data protection lawsuit seeking compensation under UK data protection laws.

If the information used in a doxing incident is considered 'personal data' under Article 4(2) of the UK GDPR, the victim may be able to file a lawsuit if data protection laws were violated. If information about someone else counts as personal data, the individual may have a claim that their identifiable information was unlawfully disclosed. If the victim suffers physical or emotional distress because of the doxing, the compensation amount may be significantly increased. In the United Kingdom, individuals can seek compensation for a breach of privacy if their right to control their private information is violated. Article 8 of the European Convention on Human Rights states that a person's private and family life, home, and correspondence must be respected. Courts in the United Kingdom have interpreted the right to privacy to include the misuse of private information. If someone shares personal information on a public platform, there is a reasonable expectation that it will remain private and protected under Article 8 of the ECHR. The Computer Misuse Act of 1990 also criminalizes unauthorized access to a computer or computer system to obtain information for doxing.

4. Doxing Cases Raised in India

4.1. Rana Ayyub Case

Rana Ayyub, an award-winning investigative journalist and vocal critic of the Indian government, has become a high-profile victim of doxing, highlighting the lack of legal protections against such harassment in India. Ayyub rose to fame through her investigative journalism, exposing government complicity in the 2002 Gujarat riots. She has faced relentless online abuse, threats, and multiple instances of doxing. Doxing involves sharing an individual's private information online without consent, often to intimidate or harm them. The scenario worsened when a highly realistic but pornographic video featuring Ayyub started going viral online. Although the video was quickly exposed as a hoax, the harm had already been inflicted. The video, along with the exposure of her private details, put Ayyub in a precarious situation. She was bombarded with hateful calls and messages, some even threatening violence against her and her family. The threats extended beyond the digital world, with some individuals threatening her physical well-being, claiming to know her residence.

Ayyub herself has described the ordeal as “emotionally crushing.” She felt unsafe even in her own house and had to seek temporary shelter to protect herself. Despite lodging complaints with the authorities and speaking out about the abuse publicly, she found few legal options available to her because India lacks specific laws against doxing. In Ayyub's case, her personal details were widely circulated online, leading to threats and intimidation. Despite filing complaints and speaking out, the lack of specific anti-doxing laws in India limited her legal recourse. Existing laws, such as the IPC and the IT Act, offer some protection but are not always effective in addressing doxing. Challenges in seeking justice include law enforcement's lack of expertise in investigating online harassment and slow responses from social media platforms. Ayyub's case drew international attention, with organizations such as the United Nations calling for stronger protections for journalists facing online harassment. The need for stronger legal protections against doxing in India is urgent, with the Personal Data Protection Bill offering hope for more comprehensive privacy safeguards. Specific legislation criminalizing doxing and holding perpetrators accountable is essential to prevent further harassment and intimidation online.

4.2. Pegasus Spyware Scandal

The Pegasus Spyware scandal, named after the software developed by NSO Group, exposed unauthorised surveillance and privacy breaches targeting journalists, activists, politicians, and other prominent figures worldwide. This incident also highlighted the malicious practice of doxing, which involves revealing private information without consent. Pegasus is a highly sophisticated spyware, initially marketed to combat terrorism and crime. However, it was frequently used for political surveillance, targeting thousands of individuals in various countries. In India, over 300 phone numbers were identified as potential targets, including those of journalists, activists, and opposition politicians. The Pegasus paper, coordinated by Forbidden Stories and Amnesty International, revealed the extent of this surveillance operation. In India, this scandal raised concerns about doxing and the potential misuse of personal information for political purposes. Surveillance technologies like Pegasus can easily weaponize personal data, leading to intimidation, harassment, or discrediting of individuals. Doxing can have severe consequences, including discrediting public figures, stifling free speech, and issuing physical threats. In India, journalists, activists, and opposition leaders were potential targets, making them vulnerable to smear campaigns and physical violence. The legal implications in India are significant. While the right to privacy is recognized, laws such as the IT Act and the proposed Personal Data Protection Bill are inadequate to address the complexities of modern digital threats, including Pegasus. Specific legislation to combat doxing and better regulation of surveillance technologies are essential. It revealed the urgent need for stronger legal protections against unauthorized surveillance and doxing. Comprehensive privacy laws and specific legislation to combat doxing are essential to safeguard individuals' rights in the digital age.

4.3. #MeToo Movement

The #MeToo movement gained traction in India in 2018, allowing women to share stories of harassment and abuse. However, it also highlighted the controversial practice of doxing, the public sharing of personal information without consent, which raised ethical and legal concerns. During the movement, individuals accused of sexual misconduct were publicly named and doxed, leading to debates about privacy, defamation, and the presumption of innocence. The right to privacy clashed with the movement's goal of public accountability, prompting debates over the right to be forgotten and the need for legal protections. Ethical considerations surrounding doxing included balancing privacy and accountability, the presumption of innocence, potential for false accusations, and chilling effects on free speech. Legal responses in India, such as the IT Act and the IPC, were not comprehensive enough to address modern digital privacy violations. The proposed Personal Data Protection Bill aimed to regulate personal data and privacy, but its implementation remained uncertain. The conflict between privacy rights and public accountability in the digital age continues to pose challenges in India, highlighting the need for clear legal frameworks to address doxing concerns while ensuring justice for survivors of harassment and abuse.

4.4. Communal Targeting through Doxing

Doxing, a prevalent form of harassment, has been used to target specific communities in India. The “Sulli Deals” incident in 2021 exposed Muslim women to severe harassment by sharing their pictures and personal details without consent. This case

highlighted the growing threat of communal targeting and inadequacies in India's legal and technological framework. The "Sulli Deals" app showcased Muslim women for a fake auction, violating their privacy and targeting journalists, activists, and professionals. The app seemed politically motivated, coinciding with rising tensions between India's Hindu majority and Muslim minority. Following widespread outrage, Delhi Police registered an FIR under Sections 302 of the IPC and the IT Act and arrested some individuals involved. The incident brought into focus the role of technology platforms like GitHub, which were criticized for allowing the app to be hosted and distributed. The lack of proactive measures by tech companies enables the spread of abusive content, and the legal grey area allows platforms to act only after harmful content has been uploaded and reported.

The absence of a specific law addressing doxing makes it difficult for victims to seek justice. India's existing laws, such as the IT Act, are outdated in the context of modern cybercrimes. The Personal Data Protection Bill lacks specific provisions to deal with doxing and targeted online harassment. The "Sulli Deals" incident had a chilling effect on the safety of women and minorities in India's digital space. Muslim women have been frequent targets of online hate campaigns. The incident is reflective of a larger trend of online communalism, where social media platforms are increasingly being used to spread hate speech and target minority communities. The failure to regulate these platforms effectively has allowed hate speech and harassment to flourish. The government must prioritize the creation of robust cybersecurity laws that protect the rights of individuals, particularly women and minorities, from online harassment. Technology platforms must be held to higher standards of accountability to prevent the spread of harmful content.

4.5. Recommendations for Enforcing Doxing Laws in India

- Define Doxing in Legislation - Ensure the law clearly defines doxing as the unauthorised disclosure of personal information, such as names, addresses, and phone numbers.
- Establish a Unique Crime for Doxing: a specific law that criminalizes doxing, with defined punishments including heavy fines and jail time for those found guilty.
- Improve Support for Victims - Set up a special hotline for people who have been doxed to report incidents and receive immediate help, and offer legal support and counseling to help victims address legal issues. Develop guidelines for police forces on handling doxing cases with care and consistency.
- Require Online Platforms to Have Reporting Systems - Make it mandatory for online platforms to have robust reporting systems for doxing cases, and demand that these platforms have clear rules for quickly removing harmful content and making it easy for users to report issues.
- Increase Digital Literacy and Awareness - Start educational programs aimed at schools, colleges, and the public to increase understanding of doxing and online privacy, and provide tools and knowledge through digital literacy initiatives to help people protect their personal data online.
- Promote Cooperation Among All Parties - Encourage teamwork among the government, police, non-profit groups, and tech companies, and hold frequent discussions and training sessions to exchange ideas and create a unified approach to tackle online abuse.
- Use Technology for Prevention - Allocate resources to develop technology to detect and stop doxing, such as software to identify and flag dangerous content on social media, and to enable continuous monitoring and removal of harmful content before it escalates into harassment.

5. Conclusion

The practice of publicly disclosing personal, identifying details without permission is considered one of the most harmful types of online aggression. It can lead to severe outcomes for those affected, including identity theft, harassment, physical threats, and psychological distress. This issue is worsened by the internet's widespread availability and social media platforms, which make it easy for doxers to share private information with large groups. In India, as in many other regions worldwide, the legal system for addressing doxing is still evolving. India currently lacks dedicated laws against doxing, though the IT Act, 2000, along with the Intermediary Guidelines and the Digital Media Ethics Code Rules, 2021, offer some legal recourse. The IT Act, specifically S. 79, provides social media platforms with "safe harbor" protection from legal action for content posted by others, provided they take appropriate measures and respond promptly to reports of illegal content. However, the rules and regulations regarding intermediaries' liability differ significantly from those in the United States, where the Communications Decency Act (CDA) S. 230 offers platforms much broader protection. In India, failure to comply with requests to remove content within a specified timeframe can result in intermediaries losing their legal defenses. The increase in doxing incidents has highlighted the urgent need for stronger protections for digital privacy. India's legal system is currently navigating challenges related to online anonymity, freedom of expression, and privacy rights. In *Puttaswamy v. Union of India* 2017, which recognized privacy as a fundamental right under Article 21 of the Indian Constitution, has set an important precedent in this area. The judgment

emphasizes the significance of individual freedom, the safeguarding of personal data, and the state's role in protecting citizens' privacy in the digital age.

Although the case did not specifically address doxing, the principles established therein could serve as a basis for future legal action against online harassment and doxing. The lack of clear jurisdiction and enforcement mechanisms further complicates the legal issues surrounding doxing. Given that the internet knows no borders, incidents of doxing often involve perpetrators and victims from different countries, complicating the process of bringing offenders to justice. Even within India, there is a pressing need for clearer and more specific laws to address the complexities of doxing. Currently, victims of doxing in India must rely on a mix of existing legislation, such as S. 354D of the IPC (stalking), S.S 499 and 500 (defamation), and S.S 66E and 67 of the IT Act (regarding non-consensual sharing of images and obscene content). These laws address aspects of the broader issue but do not provide a comprehensive approach to doxing specifically. Recent doxing cases in India have highlighted the gaps in existing laws. For instance, the Delhi High Court has been involved in cases where personal information was maliciously shared online, often leading to harassment or threats. Despite the absence of a dedicated doxing law, the courts have invoked privacy principles, directing social media platforms to take down such content and urging law enforcement to investigate the perpetrators. However, the anonymity of the internet remains a major obstacle, as identifying the individuals responsible for doxing can be challenging. In response to the growing concerns around privacy and online safety, India is currently drafting the Digital India Act, which aims to replace the outdated IT Act of 2000.

This new legislation is expected to address doxing and other forms of cyber harassment more directly, while also imposing stricter data protection measures. Until such a law is enacted, victims of doxing in India will have to rely on a patchwork of existing legal provisions to seek justice. The issue of doxing also highlights the role of social media platforms and the need for responsible content moderation. While platforms argue that they cannot be held accountable for every piece of user-generated content, there is growing recognition of their role in enabling or preventing online abuse. In India, platforms are required under the IT Rules, 2021, to appoint grievance officers and ensure clear processes for users to report harmful content. The debate over intermediary liability is far from settled, with questions about the balance between free speech and user safety remaining at the forefront of discussions both in India and globally. It is necessary to address doxing, a complex and evolving challenge that demands stronger legal and policy frameworks. In India, while existing laws offer some recourse to victims, there is a pressing need for more specific legislation that directly addresses the unique harms caused by doxing. The Puttaswamy judgment has laid the groundwork for recognising privacy as a fundamental right, but translating that into effective protection against doxing requires further legislative and judicial developments. As India continues to modernize its digital laws through the Digital India Act, it must ensure that platforms are held accountable for preventing and addressing doxing incidents while also respecting users' privacy and free speech rights. Only through a combination of legal reforms, robust enforcement, and greater public awareness can the growing menace of doxing be effectively curbed.

Acknowledgment: N/A

Data Availability Statement: The datasets and materials used in this study are available from the corresponding author upon reasonable request, subject to applicable ethical and privacy requirements.

Funding Statement: No external funding or financial assistance was received for the conduct of this research or the preparation of this manuscript.

Conflicts of Interest Statement: The authors confirm that there are no conflicts of interest associated with this study.

Ethics and Consent Statement: This research was conducted in accordance with established ethical guidelines and received approval from the relevant institutional ethics review board.

References

1. A. Cheung, "Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon," in *Handbook of Technology-Facilitated Violence and Abuse*, *Emerald Insight*, 2021. [Accessed by 01/04/2025].
2. A. Mohanty, "Critical Outlook of Doxing in India: Laws & Prevention," *Law Insider*, 2022. [Accessed by 01/04/2025].
3. V. Verma, "Legal Analysis of Doxing," *iPleaders*, 2021. [Accessed by 03/04/2025].
4. India Code, "The Indian Penal Code, 1860, Section 354(c)," *Government of India*, 1860. [Accessed by 05/04/2025].
5. India Code, "The Indian Penal Code, 1860, Section 354(d)," *Government of India*, 1860. [Accessed by 05/04/2025].
6. India Code, "The Indian Penal Code, 1860, Section 499," *Government of India*, 1860. [Accessed by 05/05/2025].
7. India Code, "The Information Technology Act, 2000, Section 66C," *Government of India*, 2000. [Accessed by 10/04/2025].

8. India Code, "The Information Technology Act, 2000, Section 66E," *Government of India*, 2000. [Accessed by 11/04/2025].
9. India Code, "The Information Technology Act, 2000, Section 67," *Government of India*, 2000. [Accessed by 11/04/2025].
10. A. K. Sikri, "Justice K.S. Puttaswamy (Retd.) v. Union of India, AIR 2018 SC (Supp) 1841," *Supreme Court of India*, 2018. [Accessed by 13/04/2025].
11. P. M. Singh, "Shaviya Sharma vs. Squint Neon, CS(OS) 134/2024," *Delhi High Court*, 2024. [Accessed by 13/04/2025].
12. United Nations, "Universal Declaration of Human Rights," *United Nations*, 1948. [Accessed by 15/04/2026].
13. United Nations, "International Covenant on Civil and Political Rights," *United Nations*, 1976. [Accessed by 15/04/2025].
14. European Union, "Regulation (EU) 2016/679 (General Data Protection Regulation)," *European Union*, 2016. [Accessed by 15/04/2025].
15. European Union, "Digital Services Act, Regulation (EU) 2022/2065," *European Union*, 2022. [Accessed by 15/04/2025].
16. France, "Code pénal, Article 223-1," *Legifrance*, 2011. [Accessed by 16/04/2025].
17. California Legislature, "California Penal Code, § 653.2," *FindLaw.com*, 2025. [Accessed by 16/04/2026].
18. California Legislature, "California Government Code, § 6218.01," *FindLaw.com*, 2025. [Accessed by 18/04/2026].
19. Texas Legislature, "Texas Penal Code, § 42.074," *FindLaw.com*, 2024. [Accessed by 18/04/2025].
20. United States Congress, "Communications Decency Act, 47 U.S.C. § 230," *Cornell Law School*, 1996. [Accessed by 18/04/2025].
21. Electronic Frontier Foundation, *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096 (9th Cir. 2009), *EFF*, 2009. [Accessed by 20/04/2025].
22. Government of India, "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules," *Ministry of Electronics and Information Technology*, 2023. [Accessed by 20/04/2025].
23. Government of India, "Bharatiya Nyaya Sanhita Bill, 2023, Sections 78 and 356," *Ministry of Home Affairs*, 2023. [Accessed by 20/04/2025].
24. Government of India, "Indecent Representation of Women (Prohibition) Act," *Indiacode*, 1986. [Accessed by 20/04/2025].
25. Government of India, "Information Technology Act, 2000, Sections 66E and 67," *Indiacode*, 2000. [Accessed by 20/04/2025].
26. United Kingdom, "Online Safety Act," *legislation.gov.uk*, 2023. [Accessed by 25/04/2025].
27. United Kingdom, "Protection from Harassment Act," *legislation.gov.uk*, 1997. [Accessed by 25/04/2025].
28. United Kingdom, "Malicious Communications Act," *legislation.gov.uk*, 1988. [Accessed by 25/04/2025].
29. GDPR, "UK General Data Protection Regulation, Art. 4(2)," *gdpr-info.eu*, 2018. [Accessed by 27/04/2025].
30. Council of Europe, "European Convention on Human Rights, Article 8," 1950. [Accessed by 27/04/2025].
31. United Kingdom, "Computer Misuse Act," *legislation.gov.uk*, 1990. [Accessed by 27/04/2025].
32. H. J. Mai and A. Martínez, "Rana Ayyub fights for press freedom in India despite harassment and death threats," *NPR*, 2023. [Accessed by 28/04/2025].
33. J. Tidy, "Pegasus: Spyware sold to governments 'targets activists'," *BBC News*, 2021. [Accessed by 28/04/2025].
34. The Times of India, "MeToo movement: Sexual harassment allegations so far," *The Times of India*, 2018. [Accessed by 28/04/2025].
35. K. Girdhar, A. Anushka, D. Khushi, N. Pakal, and S. Patodia, "Pandemic within a Pandemic: Impact of COVID-19 on Gender based Digital Violence," *International Journal of Research Publication and Reviews*, vol. 2, no. 9, pp. 294-304, 2021.

Publisher's Note: The publisher remains impartial concerning jurisdictional claims in published maps and institutional affiliations. Responsibility for the content rests entirely with the authors and does not necessarily reflect the publisher's perspectives.