
CRIMINALISATION OF ONLINE HARASSMENT AND DOXXING: NEED FOR A NEW LEGAL FRAMEWORK

Nagaraja M, SRM Institution of Science and Technology

ABSTRACT

The rise of digital platforms has turned online harassment, and doxxing in particular (the malicious publication of a person's private or identifying information without consent), into a serious threat to privacy, dignity and personal safety. Its victims are often women, journalists, activists and members of marginalised groups, who endure stalking, threats, reputational damage, loss of livelihood and psychological harm, with consequences that frequently spill into the physical world. Indian law offers no direct response to this conduct: remedies are scattered across the Bharatiya Nyaya Sanhita, 2023 (its provisions on stalking, criminal intimidation, defamation and insulting the modesty of a woman), the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, yet none of these defines or penalises doxxing as a distinct offence. These provisions are also poorly suited to anonymous and cross-border perpetrators, coordinated group attacks, the speed at which harmful content spreads, and the burden placed on victims who must pursue takedowns from platforms. This paper critically examines the existing framework and the judicial response to online harassment, exploring the conceptual and constitutional tensions between the right to privacy under Article 21 and freedom of speech under Article 19(1)(a). It also compares approaches in the United Kingdom, the United States, Australia and Singapore, several of which have enacted specific harassment or doxxing provisions, and argues that India's current patchwork leaves significant gaps in definition, enforcement and victim protection.

1. Introduction:

The internet has changed how people communicate, organise and express dissent. It has also given individuals new ways to hurt one another at scale. Online harassment, which includes cyberstalking, threats, abusive campaigns, impersonation and non-consensual sharing of intimate content, is now an everyday experience for many users. Doxxing is among its most dangerous forms. It means collecting and publishing a person's private or identifying information, such as a home address, phone number, workplace, family details or financial data, without consent and usually with the intent to intimidate, shame or expose them to harm. Its effect is to turn online hostility into a real physical threat. Once such information is released, the victim loses control over who sees it and how it is used, and the damage is often impossible to undo.

The harm goes well beyond embarrassment. Victims commonly report anxiety, withdrawal from public life, loss of employment, forced relocation and, in serious cases, physical attacks. Women, journalists, activists, and religious and sexual minorities are disproportionately targeted. Doxxing therefore also has a chilling effect on participation in public debate, which makes it a democratic concern as well as a private injury.

Indian law has no offence that squarely addresses this conduct. Victims must rely on a patchwork of provisions: the Bharatiya Nyaya Sanhita, 2023, which covers stalking, criminal intimidation, defamation and offences against the modesty of women; the Information Technology Act, 2000, with provisions such as Section 66E on violation of privacy and Section 67 on obscene content; and the Digital Personal Data Protection Act, 2023, which regulates the processing of personal data but is not designed as a penal remedy against harassment. The Supreme Court's decision in *Shreya Singhal v. Union of India* (2015), which struck down Section 66A, removed a broad and vague provision, and nothing comparable has replaced it. The recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy v. Union of India* (2017) strengthens the constitutional case for protection, but it has not produced a statute that defines and penalises doxxing.¹

¹Constitution of India, arts. 19(1)(a), 19(2) and 21; Information Technology Act, 2000, ss. 66E, 67; Digital Personal Data Protection Act, 2023.

2. Concept and Meaning of Online Harassment and Doxxing:

Online harassment refers to repeated or targeted conduct carried out through digital means that is intended to, or has the effect of, alarming, distressing, intimidating or humiliating a person. It includes cyberstalking, threats, abusive messaging, impersonation, non-consensual sharing of intimate images and coordinated pile-on campaigns. Its persistence, scale and anonymity make it more damaging than its offline counterpart. The law must still separate harassment from merely offensive or critical speech, which freedom of expression protects, by looking at targeting, repetition, intent and the effect on the victim.²

Doxxing, derived from “dropping docs”, is the intentional collection and public disclosure of a person’s private or identifying information without consent, with the purpose of harassing, intimidating or exposing that person to harm. The information may include a home address, phone number, workplace, family details or financial data. Douglas classifies doxxing as deanonymising, targeting or delegitimising, depending on whether the disclosure reveals identity, location or reputationally damaging facts.³

Doxxing is legally difficult for three reasons. The information is often individually public, so the harm lies in aggregation. It usually works by directing others to the victim, which complicates causation and liability. It also turns online hostility into physical danger, such as stalking or violence. For this reason it differs from a data breach, which is about misuse of data, and from defamation, which requires a false statement.

Not every disclosure is harmful, since journalism, whistleblowing and exposing public misconduct may involve revealing personal information in the public interest. A workable definition must therefore rest on intent, likelihood of harm, the nature of the information and the absence of a public interest justification, rather than on disclosure alone.⁴

3. Types and forms of Online Harassment and Doxxing:

The main forms of online harassment are cyberstalking, threats of violence, trolling and abusive messaging, hate speech aimed at a person’s identity, impersonation through fake

²See generally David M. Douglas, “Doxing: A Conceptual Analysis” (for a conceptual discussion of doxxing and its forms). The supplied manuscript does not provide publication details for this work.

³David M. Douglas, “Doxing: A Conceptual Analysis” (conceptual classification of doxxing as deanonymising, targeting or delegitimising). Full publication details should be added to the bibliography if available.

⁴Constitution of India, art. 19(1)(a); *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

profiles, non-consensual sharing of intimate images (including morphed images and deepfakes), online sexual harassment, and coordinated pile-on campaigns.

Doxxing falls into the following types according to what is disclosed: identity doxxing (revealing who an anonymous person is), location doxxing (a home address, workplace or movements), contact doxxing (phone numbers or email addresses), financial or official-record doxxing (bank details, government identifiers, documents), and doxxing of private images or communications.

Doxxing is also classified by method, such as hacking and data breaches, social engineering, and aggregating publicly available information, and by purpose, such as deanonymizing, targeting or delegitimising the victim.

Newer technologies are also changing these forms. Generative tools make it easy to create realistic deepfakes and synthetic intimate images, while data brokers, people-search sites and leaked databases let Criminals assemble a person's details within minutes. Swatting, where a false emergency report is made to send armed police to a victim's address, shows how doxxed information can be turned into direct physical danger. Because platforms and tools keep changing, any legal definition has to describe the harmful conduct and its effect rather than a specific technology.⁵

The motives behind these acts also shape how they should be treated. Some conduct is personal, as in revenge after a broken relationship, while other conduct is ideological, aimed at silencing journalists, activists, women in public life or members of minority communities. Some perpetrators claim to be exposing wrongdoing, which raises the public interest question discussed earlier. Distinguishing these motives matters for criminalisation, since it helps separate malicious targeting from legitimate disclosure and supports proportionate penalties.

4. Causes and Consequences of Online Harassment and Doxxing:

Online anonymity is one of the main causes of harassment. When users can hide behind pseudonyms or fake accounts, they feel less accountable and are more willing to say or do what they would not do face to face. Platform design adds to this, because algorithms that reward engagement can amplify outrage and abuse, and reporting systems are often slow, opaque or

⁵Information Technology Act, 2000, ss. 66C, 66D, 66E, 67, 67A and 67B.

inconsistent. Weak digital literacy and low awareness of privacy settings also leave users exposed, and the ready availability of personal data through social media, data breaches and people-search services makes doxxing easy.

Social and personal factors play a part as well. Gender bias, caste and religious prejudice, and political polarisation often drive the targeting of women, minorities, journalists and activists. Revenge after a personal dispute or a broken relationship is another common motive, as is the sense of belonging that comes from joining a group attack. Weak and fragmented laws, difficulty in tracing offenders and low conviction rates create a culture of impunity, so perpetrators expect few consequences.

The consequences for victims are serious and often lasting. Psychological harm includes anxiety, depression, fear, sleeplessness and loss of confidence. Doxxing adds the risk of physical danger, such as stalking, unwanted visits, swatting and violence, which may force victims to change their phone numbers, move home or live in constant fear. Victims can also suffer reputational and economic harm, including loss of employment, damaged professional prospects and the cost of security or legal help. Because content spreads quickly and is difficult to remove, the harm can continue long after the original act.

The effects reach beyond the individual. Fear of being targeted leads many people, especially women and those with unpopular views, to withdraw from online spaces or to self-censor, which has a chilling effect on free expression and democratic participation. Public trust in digital platforms and in the legal system also declines when victims see no effective remedy. These wider harms strengthen the case for dedicated legal protection.

5. Existing Legal Framework in India:

India does not have a dedicated statute on online harassment or doxxing, so victims must rely on a patchwork of general laws. The constitutional foundation lies in Article 19(1)(a), which protects free speech subject to reasonable restrictions under Article 19(2), and Article 21, which the Supreme Court in *Justice K.S. Puttaswamy v. Union of India* (2017) read to include the right to privacy and informational self-determination. At the same time, *Shreya Singhal v. Union of India* (2015) struck down Section 66A of the Information Technology Act, 2000 (IT Act) for vagueness, and no narrowly drafted replacement was enacted. Criminal liability therefore flows mainly from the *Bharatiya Nyaya Sanhita, 2023* (BNS), which replaced

the Indian Penal Code in July 2024. Its provisions on sexual harassment (Section 75), voyeurism (Section 77), stalking (Section 78), criminal intimidation (Section 351) and defamation (Section 356) are routinely stretched to cover online conduct, but they were drafted for offline settings, and several are framed around women as victims. None of them recognises the publication of a person's identifying information, such as a home address or phone number, as an offence in itself.⁶

The IT Act supplements these provisions through Sections 66C and 66D (identity theft and cheating by personation), Section 66E (violation of privacy) and Sections 67, 67A and 67B (obscene, sexually explicit and child sexual abuse material). However, Section 66E is confined to images of private areas and does not extend to textual personal data. Platforms are regulated through the safe harbour in Section 79 and the Intermediary Guidelines and Digital Media Ethics Code Rules, 2021, which require takedown of certain content on complaint but impose no criminal liability on the person who posted it. The Digital Personal Data Protection Act, 2023 gives individuals rights over their data, but it is aimed at organisations acting as data fiduciaries, relies on monetary penalties rather than criminal sanctions, and exempts processing for personal or domestic purposes, which leaves individual doxxers largely outside its reach. Courts have attempted to fill these gaps through injunctions and takedown orders, but such relief is civil, costly and inconsistent. The existing framework is thus fragmented and reactive, and it fails to address doxxing and coordinated harassment as distinct wrongs.⁷

6. Judicial Approach Towards Online Harassment and Doxxing:

Indian courts have not developed a dedicated doctrine on online harassment or doxxing. They have instead built protection case by case, drawing on constitutional principles and the general statutory provisions. At the constitutional level, *Shreya Singhal v. Union of India* (2015) set the benchmark by striking down Section 66A of the IT Act for vagueness and by insisting on a distinction between mere discussion or advocacy and incitement. This makes courts cautious about any speech-restricting provision that is loosely worded. In *Justice K.S. Puttaswamy v. Union of India* (2017), the Supreme Court recognised informational privacy as part of Article 21, and High Courts have since relied on it to protect dignity and control over

⁶Constitution of India, arts. 19(1)(a), 19(2) and 21; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

⁷Information Technology Act, 2000, ss. 66C, 66D, 66E, 67, 67A, 67B and 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Digital Personal Data Protection Act, 2023.

personal data online. In *Sri Vasunathan v. Registrar General* (Karnataka High Court, 2017) and *Subhranshu Rout v. State of Odisha* (Orissa High Court, 2020), the courts acknowledged the right to have personal information or intimate content removed from the internet, particularly in cases involving women. These decisions show a growing awareness of the permanent and compounding harm of online exposure, but they are persuasive in nature, fact-specific, and have not been consolidated into a settled legal test.⁸

In practice, relief usually comes through civil and interim remedies rather than criminal conviction. The Delhi High Court has been particularly active, granting injunctions and takedown directions against defamatory and harmful content, and in cases such as *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.* (2019) it ordered removal of online material found to be harmful to the plaintiff's reputation. Courts have also issued "John Doe" orders against unidentified wrongdoers and directed intermediaries to disclose user details or block offending links. In criminal matters, judges have stretched existing offences, such as stalking, criminal intimidation, voyeurism and defamation, to fit online conduct, while also showing concern about misuse, as seen in the Supreme Court's later insistence that police follow the safeguards laid down after the 66A decision. However, this approach has clear limits. Court-led relief is reactive, costly and uneven across jurisdictions, and it often arrives after the content has already spread. Because judges can only apply the law as it exists, they cannot criminalise doxxing as a standalone wrong or address coordinated harassment campaigns. This judicial gap strengthens the argument for a clear legislative framework.⁹

7. Challenges in Criminalising Online Harassment and Doxxing:

Criminalising online harassment and doxxing is difficult because the law must protect people from real harm without choking legitimate expression. The first challenge is definitional. Terms like "harassment", "abuse" and "offensive" are subjective, and the Supreme Court's decision in *Shreya Singhal v. Union of India* (2015) shows what happens when a provision is drafted too loosely: Section 66A was struck down because it allowed arbitrary arrests for speech that was merely annoying or unpopular. Doxxing raises an even harder question. The same piece of information, such as a name, workplace or address, may be shared

⁸*Shreya Singhal v. Union of India*, (2015) 5 SCC 1; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

⁹*Sri Vasunathan v. Registrar General*, W.P. No. of 2017 (Karnataka High Court, 2017); *Subhranshu Rout v. State of Odisha*, 2020 SCC OnLine Ori 878; *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd.*, 2019 SCC OnLine Del 8494. Verify the first case's complete case number and citation before submission.

to threaten someone, but it may also be shared by a journalist exposing wrongdoing, by a whistleblower, or by a citizen calling out a public official. A law that does not clearly separate malicious intent from public interest risks silencing dissent and investigative reporting. There is also a practical problem of proof. Offenders hide behind anonymous accounts, VPNs and foreign servers, and digital evidence is easily deleted or altered, so even a well-drafted offence may be hard to enforce. Coordinated “pile-on” campaigns add to this difficulty, since each participant may contribute only a small act, while the combined effect on the victim is devastating.¹⁰

The second set of challenges lies in implementation and institutional capacity. Police in many parts of India lack the training, tools and cyber forensic infrastructure to investigate such complaints promptly, and victims, particularly women and marginalised persons, often face dismissive responses or pressure to withdraw their complaints. Jurisdiction is another hurdle, as the offender, the victim and the platform may each be in a different state or country, which slows down requests for data and takedown. Platforms themselves are caught between their safe harbour obligations under Section 79 of the IT Act and the pressure to remove content quickly, and excessive removal can lead to private censorship. Finally, there is a real risk of misuse. Broad criminal provisions can be weaponised by powerful individuals or the State to target critics, as happened with Section 66A even after it was struck down. Any new framework must therefore balance dignity and safety against free expression, and must include clear definitions, an intent requirement, public-interest exceptions and procedural safeguards so that it protects victims without becoming a tool of oppression.

8. Comparative Analysis: Legal Frameworks in the United States and the United Kingdom:

The United States has no single federal law against online harassment or doxxing, and its approach is shaped largely by the First Amendment, which protects even offensive speech unless it falls into narrow categories such as true threats or incitement. Federal liability arises mainly through 18 U.S.C. Sec. 2261A (the federal cyberstalking statute), which criminalises a course of conduct using electronic communication that causes substantial emotional distress or places a person in fear of harm, and through 47 U.S.C. § 223, which covers harassing

¹⁰Shreya Singhal v. Union of India, (2015) 5 SCC 1 (striking down Information Technology Act, 2000, s. 66A for vagueness and overbreadth).

communications. In *Counterman v. Colorado* (2023), the Supreme Court held that a conviction for true threats requires proof that the defendant had at least a reckless state of mind, which shows how strongly American law protects speech and insists on a culpable mental element. Doxxing is addressed mostly at the state level. California, for example, enacted a statute (Penal Code § 653.2) targeting the electronic publication of personal information with intent to incite harassment, and several other states have passed similar laws, while a federal bill, the Online Safety Modernization Act, has been proposed without success. Platforms are largely shielded by Section 230 of the Communications Decency Act, 1996, which protects intermediaries from liability for third-party content, so victims rely on platform policies rather than legal compulsion. The American model offers strong free-speech safeguards and an emphasis on intent, but it is fragmented, varies from state to state, and leaves many doxxing victims without a uniform remedy.¹¹

The United Kingdom takes a more statutory and victim-focused approach. The Protection from Harassment Act 1997 criminalises a course of conduct amounting to harassment or stalking, and it applies to online behaviour. The Malicious Communications Act 1988 and Section 127 of the Communications Act 2003 have historically penalised grossly offensive or threatening messages, although these provisions drew criticism for breadth and have been replaced in part by the Online Safety Act 2023, which created new communications offences, including false, threatening and harmful communications, and the offence of sending messages intended to cause serious distress. The Act also places duties of care on platforms, enforced by the regulator Ofcom, which can impose heavy fines for failing to address illegal content. Doxxing is not a standalone offence in England and Wales, but it can be prosecuted under harassment, stalking or data protection law, and the Data Protection Act 2018 provides an offence of unlawfully obtaining or disclosing personal data. Compared with the United States, the UK offers more uniform national protection and stronger platform accountability, but it has faced concern that broad communication offences may chill free expression. For India, both models are instructive: the US underlines the importance of intent and narrow drafting, while the UK shows the value of a unified statutory scheme combined with regulatory oversight of platforms.¹²

¹¹18 U.S.C. § 2261A; 47 U.S.C. § 223; *Counterman v. Colorado*, 600 U.S. 66 (2023); Cal. Penal Code § 653.2; Communications Decency Act, 47 U.S.C. § 230.

¹²Protection from Harassment Act 1997 (UK); Online Safety Act 2023 (UK); Data Protection Act 2018 (UK); Communications Act 2003, s. 127 (UK). Check the current status and application of the communications

9. Need for a New Legal Framework in India:

India needs a new legal framework because the laws we rely on today were never built for the kind of harm people face online. Imagine someone's home address, phone number and workplace being posted on social media so that strangers can target them. Under the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000, that act of exposure is not an offence in itself. Victims have to squeeze their situation into other offences such as stalking, criminal intimidation or defamation, and each of these asks for additional elements while ignoring the real wrong, which is the exposure of personal information. Section 66E of the IT Act protects only images of private areas, and the Digital Personal Data Protection Act, 2023 is aimed at organisations and relies on monetary penalties, so an individual doxxer often slips through. Many existing provisions are also written with women as the only victims, which leaves men, transgender and non-binary persons with little direct protection. Ever since *Shreya Singhal v. Union of India* (2015) struck down Section 66A, no carefully drafted replacement has been introduced, so the law keeps leaning on provisions designed for the offline world. Mass pile-on campaigns make the problem worse: each person's contribution may look small, yet together they can destroy someone's peace of mind. Courts have stepped in with injunctions and takedown orders, but this relief is costly, uneven and often arrives after the damage is done.¹³

What India needs, then, is a dedicated law that is clear, fair and balanced. It should define doxxing and aggravated online harassment in gender-neutral language, require an intention to harass, threaten or harm, and protect journalism, whistleblowing and honest criticism through express public-interest exceptions, so that it meets the standards of clarity and proportionality set in *Shreya Singhal* and *Justice K.S. Puttaswamy v. Union of India* (2017). It should recognise coordinated harassment and prescribe stronger penalties where the victim is a child, a woman or someone otherwise vulnerable. Just as importantly, the law should put the victim first, with quick takedown of content, interim protection orders, anonymity during proceedings and compensation, along with clear duties and deadlines for platforms. Better police training, stronger cyber forensic capacity and smoother coordination between states are equally essential, as is a set of safeguards to stop the law from being misused against critics. By learning from the United States, which stresses intent and narrow drafting, and from the United

offences before final submission.

¹³Information Technology Act, 2000, s. 66E; Digital Personal Data Protection Act, 2023; Bharatiya Nyaya Sanhita, 2023, ss. 75, 77, 78, 351 and 356.

Kingdom, which pairs statutory offences with platform regulation, India can create one unified law that protects dignity and privacy without weakening free speech.¹⁴

10. Recommendations and Suggestions:

India should begin with the law itself. A dedicated statute, or a focused amendment to the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000, should name doxxing and aggravated online harassment as distinct offences, so that victims no longer have to squeeze their cases into stalking, intimidation or defamation. The definitions should be clear and gender-neutral, protecting men, women, transgender and non-binary persons alike, and should require a genuine intention to harass, threaten or harm. Journalism, whistleblowing and honest criticism must be protected through public-interest exceptions, while coordinated harassment and attacks on children, women or high-risk persons such as journalists and activists should attract stronger penalties. Punishments should stay proportionate so that the law does not become excessive.¹⁵

Equally important is how the law works in practice. Victims need quick relief, including fast takedown of content, interim protection orders, anonymity, compensation and access to counselling and legal aid. Platforms should have fixed timelines to act on complaints and preserve evidence, with an independent grievance mechanism to prevent both inaction and over-removal. Police and judges need regular training on cyber offences, and every state should have a well-equipped cyber cell working with the Indian Cyber Crime Coordination Centre (I4C). Awareness programmes in schools and colleges can help prevent harm before it happens, and safeguards such as preliminary scrutiny before arrest and transparency reporting will keep the law from being misused.¹⁶

11. Conclusion:

Online harassment and doxxing have turned the internet into a place where a person's privacy, safety and dignity can be lost within minutes. India's existing laws, from the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000 to the Digital Personal Data

¹⁴Shreya Singhal v. Union of India, (2015) 5 SCC 1; Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

¹⁵Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000; Constitution of India, arts. 19(1)(a), 19(2) and 21.

¹⁶Information Technology Act, 2000, s. 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Protection Act, 2023, offer some protection, but they were never designed to deal with the exposure of personal information or with coordinated online abuse. Courts have tried to fill the gaps, yet their relief is often slow, costly and reactive. The experience of the United States and the United Kingdom shows that a good law needs clear definitions, a requirement of intent and a sensible role for platforms.¹⁷

India therefore needs a dedicated, gender-neutral and carefully drafted framework that treats doxxing and aggravated harassment as distinct offences, protects journalism and honest criticism, and puts the victim's safety and quick relief first. Such a law, backed by trained police and accountable platforms, can protect dignity and privacy while keeping free speech intact.¹⁸

¹⁷Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000; Digital Personal Data Protection Act, 2023.

¹⁸For comparative reference, see Protection from Harassment Act 1997 (UK), Online Safety Act 2023 (UK), 18 U.S.C. § 2261A, and Cal. Penal Code § 653.2.

REFERENCES:

A. Legislation

- The Constitution of India, Arts. 19(1)(a), 19(2) and 21.
- Bharatiya Nyaya Sanhita, 2023.
- Information Technology Act, 2000.
- Digital Personal Data Protection Act, 2023.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- Protection from Harassment Act, 1997 (UK).
- Online Safety Act, 2023 (UK).
- Communications Decency Act, 1996 (US).

B. Cases

- Shreya Singhal v. Union of India, (2015) 5 SCC 1.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Sri Vasunathan v. Registrar General, Karnataka High Court (2017).
- Subhanshu Rout v. State of Odisha, 2020 SCC Online Ori 878.
- Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd., 2019 SCC Online Del 8494.
- Counterman v. Colorado, 600 U.S. 66 (2023).

C. Bibliography

- Douglas, David M., *Doxing: A Conceptual Analysis*.
- Research articles on online harassment, cyberstalking, doxxing and digital privacy.
- Scholarly articles examining freedom of speech under Article 19(1)(a) and the right to privacy under Article 21.
- Comparative studies on cyber harassment legislation in India, the United States and the United Kingdom.