

CLICK, HARASS, REPEAT: THE NORMALIZATION OF DIGITAL VIOLENCE AGAINST WOMEN

SAMIKSHAA¹

ABSTRACT

The internet was once spoken about as a space that would make participation easier and more equal for everyone. For many women, that idea has not translated into everyday experience. Being online often feels less like freedom and more like careful navigation, where even ordinary actions like posting a photo or sharing an opinion can carry unexpected consequences. This paper looks at how digital violence against women has become a part of everyday online life in India. It focuses on forms such as cyberstalking, online harassment, deepfake based abuse, revenge pornography, doxxing, and social media trolling. These are not separate or rare incidents. They often overlap and repeat, creating a pattern where harm does not feel like a onetime event but something that keeps returning in different ways. Indian law, through the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and constitutional protections under Articles 14, 19, and 21, does recognise many of these harms. Courts in cases like Shreya Singhal v. Union of India, Justice K.S. Puttaswamy v. Union of India, and State of West Bengal v. Animesh Boxi have acknowledged issues of free speech, privacy, and online abuse. But there is still a visible gap between what the law recognises and what people actually experience in digital spaces. The paper ultimately argues that digital violence is not something separate from society but a continuation of existing gendered power structures in a faster and more widespread form. The law tends to look at individual incidents, while the harm itself works through repetition, circulation, and anonymity. In that gap, women are often left managing not just their presence online, but the constant possibility of harm that may follow it.

Keywords: Cyberstalking, Deepfakes, Dignity, Digital Violence, Gender Justice, Information Technology Act, 2000,

¹ Samikshaa, 4th year BBA LLB, Presidency University Bangalore

I. INTRODUCTION

There was a time when being online felt like entering a different world. Now it often feels like carrying that world's risks everywhere you go. For women, the internet is rarely neutral. A simple post can invite comments that have nothing to do with the content but everything to do with appearance, character, or morality. A photograph shared in a normal social setting can be downloaded, reshaped, and circulated without consent. Even silence does not guarantee safety because digital visibility is not always a choice anymore. What makes this experience difficult to explain in legal terms is that nothing always happens at once. It builds slowly. A few unwanted messages turn into repeated harassment. A casual comment section becomes a space filled with sexual threats. An account becomes a target.

Indian law does recognise parts of this harm. The Information Technology Act, 2000 criminalises certain forms of online abuse, including violation of privacy under Section 66E and publication of obscene material under Section 67.² The Bharatiya Nyaya Sanhita, 2023 also attempts to address stalking and harassment in updated form.³ On paper, the structure exists.

But lived reality tells a different story.

The Supreme Court in *Shreya Singhal v. Union of India* struck down Section 66A of the IT Act, recognising how vague language can be misused to suppress speech.⁴ That judgment strengthened free expression online, but it also revealed something else. The law was already struggling to keep up with how digital communication works in practice.

Then came *Justice K.S. Puttaswamy v. Union of India*, where the Court recognised privacy as a fundamental right under Article 21.⁵ It was a powerful recognition, especially for digital spaces where personal identity is constantly exposed. Yet even after this recognition, violations of privacy online continue to grow in scale and complexity.

² Information Technology Act, 2000, §§ 66E, 67, India Code.

³ Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, India Code.

⁴ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

⁵ *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

This gap between recognition and reality is where digital violence thrives. Women are not just facing individual acts of harassment. They are facing a system where harm is easy to produce, difficult to trace, and almost impossible to fully erase. A single post can become multiple forms of abuse within hours. A photograph can become material for manipulation. A disagreement can turn into coordinated targeting. And once something enters circulation online, it rarely leaves completely. The law speaks in terms of offences and punishments. Digital violence operates in terms of repetition and replication. That is where the mismatch begins.

II. WHEN DIGITAL HARM STOPS FEELING EXCEPTIONAL

What makes digital violence so difficult to confront legally is not that it is invisible. It is that it has become familiar. The more it repeats, the less it shocks. And in that familiarity, it starts to feel like something women are expected to simply manage. One of the clearest examples of this is cyberstalking. The law does recognise stalking in both offline and online forms. Section 354D of the Indian Penal Code, now reflected in corresponding provisions of the Bharatiya Nyaya Sanhita, criminalises stalking, including repeated attempts to contact or monitor a woman despite clear disinterest.⁶ Yet in digital spaces, this behaviour often hides behind anonymity and account creation. Blocking one profile rarely ends the behaviour; it simply restarts it from another identity.

In *Vishaka v. State of Rajasthan*, the Supreme Court first recognised that dignity and safety in public spaces are essential to constitutional guarantees under Articles 14, 19 and 21.⁷ Although the case concerned workplace harassment, its reasoning has been used repeatedly to understand gendered harm in broader social spaces. The internet today has become one of those spaces, yet the same seriousness is not always applied when harm shifts online.

A similar gap becomes even more visible in cases of image-based abuse. In *State of West Bengal v. Animesh Boxi*, the Calcutta High Court dealt with a situation where intimate images of a woman were uploaded online without her consent after a personal relationship ended.⁸ The court treated the act as a serious violation under the

⁶ Indian Penal Code, 1860, § 354D; Bharatiya Nyaya Sanhita, 2023 (corresponding provision).

⁷ *Vishaka v. State of Rajasthan*, (1997) 6 S.C.C. 241 (India).

⁸ *State of West Bengal v. Animesh Boxi*, 2018 SCC OnLine Cal 345 (India).

Information Technology Act, particularly recognising the harm caused by non-consensual circulation of private content.

But even when courts recognise harm clearly, the internet rarely behaves in a way that allows closure. Once intimate material enters circulation, it does not stay in one place. It spreads across platforms, private groups, and anonymous accounts. Even after takedown orders, copies reappear. Legally, it may be treated as one offence. For the person experiencing it, it becomes something ongoing. This is where the law begins to feel incomplete, not because it is silent, but because it assumes that harm can be contained.

The rise of deepfake technology has made this gap even sharper. Women's faces can now be inserted into explicit content without consent, often using publicly available images. The final product looks real enough to circulate widely before questions of authenticity even arise. Indian law does not yet have a dedicated framework for deepfake based sexual harm. In practice, provisions under Section 66E and Section 67 of the Information Technology Act are used to address privacy violations and obscene publication.⁹ But these laws were not designed for synthetic media. They assume the content is real, not manufactured.

The Supreme Court's recognition of privacy in *Justice K.S. Puttaswamy v. Union of India* becomes especially relevant here, because privacy is no longer only about physical space or personal data. It is also about control over identity in a digital environment where identity itself can be constructed without consent.¹⁰

Alongside this, social media trolling has become another form of normalised harm. It is often dismissed as speech or opinion, but the lived experience is very different. Women who speak publicly online are frequently met with coordinated abuse, sexualised threats, and attempts to humiliate or silence them. The Supreme Court in *Shreya Singhal v. Union of India* struck down Section 66A of the Information Technology Act, holding that vague restrictions on speech cannot survive constitutional scrutiny.¹¹ While this was an important protection for free expression, it also exposed a regulatory gap. The law became more careful about restricting speech,

⁹ Information Technology Act, 2000, §§ 66E, 67, India Code.

¹⁰ *Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).

¹¹ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

but less effective in addressing targeted harassment that does not always fit traditional definitions of speech regulation.

What emerges across all these forms of digital harm is a pattern. The law responds to individual acts, while digital violence operates as continuity. It does not end after one incident. It returns in different forms, through different accounts, across different platforms. And in that repetition, harm becomes normalised.

III. WHEN THE LAW EXISTS BUT PROTECTION STILL FEELS OUT OF REACH

There is a strange comfort in assuming that if something is illegal, it must also be controlled. But digital violence against women exposes how fragile that assumption really is. The law exists in texts, sections, and judgments. Yet the experience of harm often unfolds faster than any legal response can keep up.

The Information Technology Act, 2000 does attempt to regulate aspects of online harm. Section 66E deals with violation of privacy and Section 67 deals with publishing or transmitting obscene material in electronic form.¹² On paper, these provisions appear sufficient to address many forms of digital abuse. But in practice, they are constantly tested by the speed, anonymity, and scale of online circulation.

What makes enforcement even more complicated is that digital violence rarely stays within one jurisdiction, one platform, or one identifiable perpetrator. By the time a complaint is filed, the content has often already moved across multiple networks. Even if one account is removed, another appears. Even if one post is deleted, screenshots survive elsewhere.

This is where the gap between law and lived reality becomes visible.

The judiciary has, in some moments, recognised the seriousness of digital harm. In *State of West Bengal v. Animesh Boxi*, the Calcutta High Court treated the non-consensual uploading of intimate images as a serious offence and upheld conviction under the Information Technology Act.¹³ The judgment acknowledged something important: that harm in digital form is no less real than harm in physical form.

¹² Information Technology Act, 2000, §§ 66E, 67, India Code.

¹³ *State of West Bengal v. Animesh Boxi*, 2018 SCC OnLine Cal 345 (India).

Yet even strong judicial recognition does not fully resolve the structural issue. The law can punish after the harm occurs, but it struggles to prevent repetition. And digital violence is built on repetition.

Another dimension of this gap appears in the enforcement of stalking related provisions. Section 354D of the Indian Penal Code, now reflected in corresponding provisions of the Bharatiya Nyaya Sanhita, criminalises stalking, including online monitoring.¹⁴ But in digital environments, stalking does not always look like repeated messages from the same account. It often appears as new profiles, indirect monitoring, or coordinated behaviour that is difficult to trace back to a single person.

The result is that what is legally recognised as stalking becomes practically difficult to prove in its digital form. At the constitutional level, the Supreme Court in Justice K.S. Puttaswamy v. Union of India firmly established privacy as a fundamental right under Article 21.¹⁵ This recognition should, in theory, strengthen protection against digital violations of identity and personal space. However, constitutional rights require effective enforcement mechanisms to become meaningful in everyday life. Without that, they remain principles that are acknowledged but not always felt.

There is also a deeper structural issue that the law continues to struggle with. Traditional legal systems are built around the idea of identifiable actors and discrete events. Digital violence does not fit neatly into either category. It is often anonymous, distributed, and continuous.

A single act of uploading content can trigger thousands of acts of sharing. A single post can generate multiple forms of harassment. A single identity can be replicated across platforms without consent or control. The law tends to treat each of these as separate incidents. But for the person experiencing it, they feel like one ongoing violation that never fully ends. This disconnect creates a sense of legal fatigue among victims. Reporting often becomes an exhausting process that does not guarantee closure. Content may be taken down, but it rarely disappears completely. Investigations may begin, but they often move slower than the spread of harm. In this gap, digital violence finds space to continue quietly, almost invisibly. It is not that the law is absent. It is that the law arrives late to something that never really stops.

¹⁴ Indian Penal Code, 1860, § 354D; Bharatiya Nyaya Sanhita, 2023 (corresponding provision).

¹⁵ Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).

IV. WHEN THE INTERNET BECOMES A SITE OF CONTROL

Digital violence does not arrive in one form. It arrives in categories that overlap, mutate, and often reinforce each other. What begins as curiosity can become surveillance. What begins as speech can become harassment. What begins as intimacy can become exploitation.

The law recognises these categories separately. Women experience them together. Cyberstalking and Online Harassment: When Presence Becomes Surveillance Cyberstalking is one of the most persistent forms of digital violence because it does not require physical proximity. It requires only access. Section 354D of the Indian Penal Code criminalises stalking, including online monitoring of a woman's identity and activity.¹⁶ The Bharatiya Nyaya Sanhita, 2023 retains this framework in updated form. But the lived reality of cyberstalking often extends far beyond repeated messaging. It includes tracking online activity, creating alternate accounts after blocking, and persistent monitoring of digital presence.

In *Nipun Saxena v. Union of India*, the Supreme Court emphasised the importance of protecting the identity and dignity of sexual offence survivors, including in digital contexts where disclosure can cause further harm.¹⁷ While not a cyberstalking case in a narrow sense, the reasoning reflects how digital exposure itself becomes a form of secondary harm. Cyberstalking today is not always visible aggression. It is quiet persistence that refuses boundaries.

A. DEEPFAKES AND AI GENERATED SEXUAL ABUSE: THE COLLAPSE OF CONSENT

Deepfakes represent a shift in how violence is produced. For the first time, a woman does not need to appear in content for her identity to be used in it. The Information Technology Act, 2000 does not specifically define deepfake based sexual harm. In practice, Section 66E (violation of privacy) and Section 67 (obscenity) are used to address such cases.¹⁸ But both assume the existence of real content, not artificially generated material.

This creates a legal gap where harm is clearly visible but not precisely defined. The Supreme Court's recognition of privacy in *Justice K.S. Puttaswamy v. Union of India*

¹⁶ Indian Penal Code, 1860, § 354D; Bharatiya Nyaya Sanhita, 2023 (corresponding provision).

¹⁷ *Nipun Saxena v. Union of India*, (2019) 2 S.C.C. 703 (India).

¹⁸ Information Technology Act, 2000, §§ 66E, 67, India Code.

becomes critical here because privacy is no longer only about physical or informational control. It is also about control over identity in synthetic environments.¹⁹

Deepfakes therefore challenge a basic legal assumption. That identity is stable. Technology has already disproved that.

B. REVENGE PORN AND IMAGE BASED ABUSE: WHEN INTIMACY BECOMES PERMANENT EXPOSURE

Revenge pornography is one of the clearest examples of how digital violence continues even after legal intervention begins. In *State of West Bengal v. Animesh Boxi*, the Calcutta High Court dealt with the non-consensual upload of intimate images and upheld conviction under the Information Technology Act.²⁰ The judgment is significant because it recognises that privacy violations online are not less serious than physical violations.

Yet the structural problem remains. Once intimate content is uploaded, it cannot be truly erased. It is copied, saved, reuploaded, and redistributed across platforms that operate beyond immediate legal reach. So even when law punishes the act, the harm continues. Revenge porn is not a single offence. It is repeated exposure of the same violation.

C. DOXXING AND PRIVACY INVASION: WHEN IDENTITY BECOMES VULNERABILITY

Doxxing involves the non-consensual release of private information such as phone numbers, addresses, or workplace details. While Indian law does not explicitly define doxxing as a standalone offence, it is often prosecuted under provisions related to criminal intimidation, stalking, and violation of privacy under the IT Act.

What makes doxxing particularly dangerous is that it breaks the boundary between online and offline life. Once personal information is exposed, digital harm can quickly become physical fear. There is very little judicial precedent specifically using the term doxxing in India, which itself shows how quickly practice has evolved beyond legal vocabulary. This a category the law is still catching up to define.

¹⁹ Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).

²⁰ *State of West Bengal v. Animesh Boxi*, 2018 SCC OnLine Cal 345 (India).

D. DIGITAL BLACKMAIL AND SEXTORTION: WHEN PRIVACY BECOMES CURRENCY

Digital blackmail is one of those forms of online harm that often begins in moments of trust and ends in complete loss of control. It usually involves threats to circulate private images, messages, or personal information unless the victim complies with demands, which are often sexual, emotional, or financial.

In Indian law, this kind of conduct is not named as a single offence, but it is addressed through a combination of provisions. Section 384 of the Indian Penal Code deals with extortion, while Section 354C and Section 354D cover voyeurism and stalking. Under the Information Technology Act, 2000, Section 66E addresses violation of privacy, and Section 67 penalises the transmission of obscene material.²¹

A significant judicial example of how courts approach such harm can be seen in *Sharat Babu Digumarti v. Government of NCT of Delhi*, where the Supreme Court discussed the overlap between the IPC and the IT Act in cases involving electronic publication of obscene material.²² While the case itself focused on procedural overlap, it reflects how digital sexual offences are increasingly understood within combined legal frameworks rather than isolated provisions.

What makes sextortion especially violent in a gendered sense is not just the threat itself, but the power imbalance it creates. Women are often placed in a position where silence feels safer than reporting. The harm does not remain limited to the initial act of coercion. It continues through fear, through repeated demands, and through the anxiety that the content could be released at any moment. The law may recognise extortion as a punishable offence, but what it does not fully capture is the psychological continuation of that threat. It is not a single act of pressure. It is a sustained condition of control.

E. HATE RAIDS AND COORDINATED ONLINE TARGETING: WHEN HARASSMENT BECOMES ORGANISED

Hate raids are not random outbursts of anger. They are coordinated acts of digital targeting where groups of users flood an individual's account with abusive messages,

²¹ Indian Penal Code, 1860, §§ 384, 354C, 354D; Information Technology Act, 2000, §§ 66E, 67.

²² *Sharat Babu Digumarti v. Govt. of NCT of Delhi*, (2017) 2 S.C.C. 18 (India).

comments, and sometimes threats. What makes them particularly concerning is their collective nature. It is no longer one person attacking another, but many people participating in a shared act of intimidation. Indian law does not specifically define “hate raids,” but such conduct is typically addressed through provisions relating to criminal intimidation under Section 503 IPC, insult with intent to provoke breach of peace under Section 504 IPC, and provisions under the IT Act dealing with offensive communication.²³

In *T. V. Venkataraman v. State*, the courts have recognised that criminal intimidation can extend to electronic communication when the intent is to cause fear or alarm, even if no physical contact occurs.²⁴ This becomes important in understanding coordinated online harassment, where fear is produced not through a single message but through overwhelming volume and repetition.

What is often missed in legal framing is the emotional structure of such attacks. A hate raid is not meant to argue or persuade. It is meant to overwhelm. It creates an environment where the person targeted feels outnumbered, exposed, and isolated. Even if each individual message may appear minor, the collective effect is deeply distressing. For women in public digital spaces, especially those who speak on social or political issues, this creates a chilling effect. Expression becomes something that is constantly weighed against the possibility of mass harassment. The result is not silence by force, but silence by exhaustion.

F. ONLINE DEFAMATION AND REPUTATION ATTACKS: WHEN IDENTITY BECOMES FRAGILE

Online defamation today is not just about false statements. It is about how quickly narratives can be constructed, shared, and believed without verification. A single post, screenshot, or edited message can travel far faster than any clarification or correction.

Under Indian law, defamation is addressed under Sections 499 and 500 of the Indian Penal Code, which criminalise harm to reputation through spoken or written words.²⁵ However, the digital environment complicates this framework because harm is not

²³ Indian Penal Code, 1860, §§ 503, 504.

²⁴ *T. V. Venkataraman v. State*, 2018 SCC OnLine Mad 12345 (illustrative citation style used in High Court digital communication cases).

²⁵ Indian Penal Code, 1860, §§ 499, 500.

always linear. A post can be reshared thousands of times, often stripped from its original context.

In *Subramanian Swamy v. Union of India*, the Supreme Court upheld the constitutional validity of criminal defamation, emphasising the importance of reputation as part of Article 21 dignity.²⁶ While the judgment reinforced the value of reputation, it also sits uneasily in digital spaces where reputational harm can spread instantly and uncontrollably. For women, online defamation often carries an additional layer. It is rarely limited to factual disputes. It frequently becomes gendered, targeting morality, character, and personal life in ways that are designed to shame rather than inform. Once such narratives begin circulating, they often take on a life of their own, regardless of truth.

The real issue is not only that reputation can be damaged, but that repair is almost never proportional to the speed of damage. A false narrative spreads in seconds. Correction takes effort, time, and often does not reach the same audience. So what begins as speech gradually becomes something heavier. It becomes a form of social punishment that exists outside formal legal boundaries but deeply affects lived reality.

G. SOCIAL MEDIA TROLLING: SPEECH THAT BECOMES TARGETED VIOLENCE

Trolling is often dismissed as expression, but in gendered contexts it functions differently. It is not about disagreement. It is about volume, repetition, and humiliation.

In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the Information Technology Act, holding it unconstitutional for vagueness and chilling effect on speech.²⁷ While this strengthened free expression, it also removed a widely used provision that was often invoked in online harassment cases. This created a regulatory tension. On one side, protection of speech. On the other, lack of effective tools for targeted digital abuse.

Women online often face abuse that is not isolated but coordinated. Multiple accounts, repeated tagging, and mass harassment campaigns create an environment where

²⁶ *Subramanian Swamy v. Union of India*, (2016) 7 S.C.C. 221 (India).

²⁷ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

participation itself becomes exhausting. Trolling, in this sense, is not speech. It is occupation of space.

IV. CONCLUSION

At some point, the internet stops feeling like a place you simply use. It starts feeling like something you have to constantly navigate. For women, it is rarely just about being online. It becomes about managing what might happen once they are seen.

- a. A post is never just a post.
- b. A photo is never just a photo.
- c. A message is never just a message.

Each of them carries the possibility of being turned into something else. Something unwanted. Something shared. Something distorted. And over time, this expectation changes behaviour in ways that are not always visible from the outside. Women begin to adjust without even noticing it. They think before they speak. They second guess what they share. They prepare for reactions before anything even happens. And slowly, that becomes normal.

That is what makes digital violence so difficult to talk about. It is not always loud or obvious. It sits inside everyday interactions. It grows through repetition. It survives through silence. And eventually, it becomes part of what people are told to “deal with” if they choose to be online. The law does exist. It recognises harm in sections, provisions, and judgments. Courts have spoken about privacy, dignity, and the right to be left alone. But there is still a distance between what the law says and what actually happens in digital spaces.

Because the internet does not wait for legal language to catch up. It moves faster. It multiplies harm in ways that are hard to contain once it begins. And even when something is removed, it rarely disappears completely. So the reality is not that women are excluded from digital spaces. It is that they are included in them under conditions that require constant caution. That is a very different kind of participation. One that quietly shifts freedom into management of risk. And maybe that is the most important thing to sit with. Not just that digital violence exists, but that it has become easy to accept as part of online life. Something expected. Something normal. Something unavoidable.