

International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham



This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Digital Moral Policing as Informal Justice: Gender Regulation, Cultural Norms, and the Limits of Law In Online Spaces

Deeptakshi Bhattacharya^a

^aHimachal Pradesh National Law University, Shimla, India

Received 20 June 2026; Accepted 20 July 2026; Published 24 July 2026

The Internet has become a space of constant surveillance and social control, and a source of new forms of social justice, such as trolling, public shaming, cyber-bullying, and "digital" vigilantism, that are based on the collective conscience and sense of morality of the community. The article contends that such moral policing takes place in the same constitutional environment wherein there is a right to free speech and a right to privacy and dignity, but mostly eludes them. Based on theories of disciplinary power by Foucault, social control by means of impression management by Goffman and feminist legal theories by Butler and MacKinnon, it is argued that India's cyber law regime, namely, IT Act 2000, Intermediary Rules 2021 and the Digital Personal Data Protection Act 2023, is structurally incapable of addressing the issues related to digital moral policing because these laws primarily aim at addressing the wrongdoing committed by identifiable individuals instead of collective and anonymous action through crowd. The piece illustrates, using the example of an Indian journalist called Rana Ayyub, the inadequacies of legal remedies and how they are often late, and that they often fail to deal with the networks that are behind such campaigns.

Keywords: *media vigilantism, media trial, informal justice, constitutional free speech, gendered digital abuse, media surveillance.*

INTRODUCTION

One particular night, Aisha, a young 21-year-old university student, posted a picture of herself on a social networking site after participating in a college festival at her university. Within hours, this image started making its rounds on various platforms along with insulting comments regarding her “character”, attire, and morals. Various anonymous people called her “shameless”, whereas some even demanded that she should be punished by her university for what she had done. Screenshots of her profile were being shared by random individuals, her contact details were revealed, and scores of comments made her part of a public moral tribunal. Nothing happened in a court of law or anything of such nature; there was no official ruling on the matter because this case couldn’t be filed in a court of law, but still the punishment was swift and harsh. Scared of further bullying and stigma, she disabled her account and stopped using any kind of social networking sites. Although a hypothetical scenario, scenarios of similar nature occur in huge numbers at any point in time in any corner of the internet. This is what the growing reality of digital moral vigilantism and media-enforced shaming appears to be.

The idea of “digital moral policing” could be seen as informal justice, since this practice is a form of punishment that is applied by Internet users for actions that are deemed to be a violation of the accepted moral rules¹. It is often used against women, members of the LGBTQ+ community, religious minorities, journalists, activists and those who have non-traditional opinions or sexualities. In situations where two or more cases occur in the online environment, the online punishments are clearly rooted in the precepts of the patriarchy and in culture during the precepts of sexuality, honour, nationalism, religion and conformity².

Judith Butler has made the claim that gender norms are socially constructed and that they are regularly and repeatedly reinforced by the expectations of society and the discipline of society³. Catherine MacKinnon has emphasised the nature of the systemic social control of women's

¹ Daniel Trottier, 'Digital Vigilantism as Weaponisation of Visibility' (2016) 30 *Philosophy & Technology* <<https://link.springer.com/article/10.1007/s13347-016-0216-4>> accessed 12 June 2026

² Pankaj et al., 'AI, GENDER AND DIGITAL JUSTICE: INVESTIGATING THE MISUSE OF INFORMATION TECHNOLOGY ACT BY WOMEN IN INDIA' (2025) 23(S3) *Lex Localis* <<https://lex-localis.org/index.php/LexLocalis/article/view/803297>> accessed 12 June 2026

³ Judith Butler, *GENDER TROUBLE: FEMINISM AND THE SUBVERSION OF IDENTITY* (1st edn, Routledge 1990)

autonomy and public involvement in patriarchal structures⁴. This issue of digital moral policing also raises a number of important legal and constitutional concerns. In India, freedom of expression and speech is guaranteed under Article 19(1)(a) of the Constitution of India along with the right to life, dignity and privacy under Article 21 of the Constitution of India⁵. The digital platforms have facilitated democratic participation but have also facilitated decentralised online vigilantism that is indistinguishable from focused harassment⁶. The Supreme Court of India has highlighted the need to reconcile the freedoms of speech with the constitutional rights to freedom from arbitrary restrictions and invasion of privacy⁷. The phenomenon thus lies in a very paradoxical milieu in the legal scenario, protected under Article 19(1)(a) of the Constitution but often violated under the vast ambit of Article 21 protecting the right to dignity, privacy, bodily integrity, and reputation⁸.

The problem with existing legislation is that it has failed to keep up with the times, since it was drafted with the assumption that the type of conduct involved in digital communications can be easily identified and is individualistic: a defamer, a stalker, an obscene distributor. Nowadays, digital moral policing takes place in the form of organisation without leadership, anonymity with organisation, jurisdictional dispersal, and platform dispersal. The Information Technology Act, 2000 and the rules made thereunder do not envision such a system; indeed, the constitutional jurisprudence that arose from *Shreya Singhal v Union of India* and the *Justice K.S Puttaswamy v Union of India* is important, but it is not as comfortable with state action as it is with horizontal harm caused by thousands of private and anonymous individuals⁹.

Sociologically, digital moral policing may be understood as an extension of informal mechanisms of social control operating within technologically mediated environments. Michel Foucault's theory of surveillance and disciplinary power explains how individuals internalise social expectations under constant observation and fear of punishment. Stigma demonstrates how

⁴ Catharine A MacKinnon, 'Feminism, Marxism, Method, and the State: An Agenda for Theory' (1982) 7(3) Signs <<https://www.jstor.org/stable/3173853>> accessed 12 June 2026

⁵ The Constitution of India 1950, arts 19(1)(a) and 21

⁶ Samina Khan et al., 'A ROUTINE ACTIVITY APPROACH TO UNDERSTANDING THE REASONS FOR TECHNOLOGY-FACILITATED HARASSMENT AGAINST WOMEN IN INDIA' (2023) 31(2) IIUM Law Journal <<https://doi.org/10.31436/iiumlj.v31i2.851>> accessed 12 June 2026

⁷ *Shreya Singhal v Union of India* (2015) 5 SCC 1; *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1 (SC)

⁸ The Constitution of India 1950, arts 19 and 21

⁹ Sapna Kumari et al., 'Impact of *Shreya Singhal v. Union of India* on Section 66A of the IT Act' (2026) 9(10) Iconic Research and Engineering Journal <<https://doi.org/10.64388/IREV9I10-1716417>> accessed 12 June 2026

public humiliation and social labelling can marginalise individuals and damage their social identity¹⁰. Online platforms amplify these dynamics by enabling mass participation in moral judgment, often without accountability or the due process of law.

The constitution marks the convergence of the constitutional right to free speech on one side and dignity and privacy on the other, thereby highlighting the inadequacies of a system of rights designed mainly for checking state action where the perpetrator is a decentralised crowd. This article attempts to show that digital moral policing constitutes an exercise in the practice of informal justice via the decentralisation of online crowds.

DIGITAL MORAL POLICING IN ONLINE SPACES

Digital moral policing refers to the informal regulation of individual conduct by online communities through practices such as trolling, slut- shaming, doxxing, cancel campaigns, and coordinated harassment, aimed at those whose conduct is perceived to violate dominant norms of gender, sexuality, religion, or political identity¹¹. The nature of policing differs from formal law enforcement as it is carried out by largely anonymous, non-state actors who assume the role of judge, jury, and executioner without any of the procedural safeguards, evidence, representation, or appeal¹².

Sociologically, digital moral policing can be seen as a form of informal justice: a method by which a community (typically the dominant communities) punishes perceived deviance, not by formal state courts but through other means. Social media platforms like Instagram (IG), Facebook, and X serve as platforms for quotidian justice, with regular users wielding quasi-judicial powers, and public 'accusation' is enough to assume guilt without any proof, facts, cross-examination or verification of facts.

This can be explained using the concept of Michel Foucault on Disciplinary Power. Foucault in *Discipline and Punish* suggested that more power is currently exercised not by centralised institutions, but rather by a constant internal sense of being observed, seen, which ultimately

¹⁰ Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Vintage 1995)

¹¹ Danielle Keats Citron, *HATE CRIMES IN CYBERSPACE* (Harvard University Press 2016)

¹² Danah Boyd, *It's Complicated: the social lives of networked teens* (Yale University Press 2014) 8–15

results in individuals policing themselves¹³. Social media mimics this state of perpetual ‘visibility’, as the comments, reposts and screenshots put them in a constant state of being looked at, and punishment is spread all over the place and not centralised in one person or state. Additionally, Erving Goffman's Theory of Stigma adds to this, since it speaks of how people with ‘deviant behaviour’ are treated with a ‘social discrediting’ which harms their identity and position in society. Stigma happens in the digital world because of widespread virality and the digital ‘always on’ nature of the experience. A common form of social punishment for people who are members of online communities is labelling them ‘immoral’ or ‘dishonourable’. Today, Internet misogyny is seen as a common aspect of Internet communication and is facilitated by other forms of media communication that marginalise and exclude women¹⁴. The stigmatising effect is further exacerbated by digital virality, as a label online will remain indefinitely and can resurface long after the initial controversy has been forgotten.¹⁵

FEMINIST LEGAL PERSPECTIVE

Till date, gender-related aspects of digital moral policing are one of the key areas of moral policing that are examined by feminist jurisprudence. These systems of social control are aimed at controlling women's bodies, sexuality, and public engagement, according to the theories developed by Butler and MacKinnon. From both Butler's and MacKinnon's theories, it is a reasonable assumption that online harassment and digital moral policing are processes that are closely linked to broader patriarchal structures in society.

According to Butler's theory on the performativity of gender, we cannot consider gender as a constant biological component of identity, but rather a process composed of several acts, behaviours, and expectations. Social structures continually reaffirm the notion of ‘acceptable’ and the ‘normal’ notions of masculinity and femininity, and anyone deviating from these ‘normal’ rules are punished. Criticism of women's body, lifestyle, dating behaviour, and even their political opinions in digital environments is a tangible illustration of the extent to which this theory, which is rooted in the socially constructed gender concept, can be strictly policed

¹³ Tarleton Gillespie, *Custodians of the Internet: platforms, content moderation, and the hidden decisions that shape social media* (Yale University Press 2018)

¹⁴ Emma A Jane, *MISOGYNY ONLINE: A SHORT (AND BRUTISH) HISTORY* (1st edn, Sage Pubns Ltd 2017)

¹⁵ Erving Goffman, *STIGMA: NOTES ON THE MANAGEMENT OF SPOILED IDENTITY* (Simon & Schuster 1986)

digitally, through the heavy policing of women's appearance, lifestyle, choice of partner, and even their political opinions.

MacKinnon also points out that patriarchy is maintained by institutionalising women's autonomy and reasserting a patriarchal norm. As MacKinnon mentioned, oppression is not a personal attack on individuals, but rather a systematic oppression perpetrated by a culture and strategic politics. These viewpoints can help make sense of why online morality policing campaigns target marginalised groups like women, queer people and minorities. Online harassment attempts to silence or punish voices of those who challenge the norms of society in public space or through their expressions of identity.

The above views from feminism are further substantiated in the literature of the modern era with regard to online misogyny. In this regard, Emma A. Jane argues that the internet has exacerbated misogynist attacks on women by normalising misogynist attacks on women online in the form of anonymous misogynist attacks¹⁶. In the same way, research on the topic of online sexism and gender related hate speech has shown that women and other marginalised groups of society that are targeted by the normative heterogeneity and subjugation of society are targeted with disproportionate threats and reputation attacks online¹⁷. These cyberbullying behaviours can be motivated by morality, honour, culture, nationalism and more.

The feminist legal perspective also highlights the link between moral policing and control of female sexuality. For centuries, honour, shame and respect have been words most commonly used and connected to the behaviour of women. Social networks are another medium through which moral policing takes place by unidentified Internet users who act embarrassingly and ruin reputations as a way of social control. Therefore, digital moral policing can be understood as the use of technology as an instrument of abuse, as well as the reproduction of gender inequalities of previous times in the present-day digital space. The two theoretical approaches, provided by Butler and MacKinnon, clearly show that digital moral policing is a gender-based process of informal justice, based on patriarchy.

¹⁶ Emma Alice Jane, "Back to the kitchen, cunt': speaking the unspeakable about online misogyny' (2014) 28(4) Continuum Journal of Media & Cultural Studies <<https://doi.org/10.1080/10304312.2014.924479>> accessed 12 June 2026

¹⁷ Aditi Dutta et al., 'Divided by discipline? A systematic literature review on the quantification of online sexism and misogyny using a semi-automated approach' (2025) 130 Scientometrics <<https://link.springer.com/article/10.1007/s11192-025-05410-2>> accessed 12 June 2026

DIGITAL VIGILANTISM

Digital moral policing is commonly seen as a form of digital vigilantism – the punishing of deviation through a process that Daniel Trottier refers to as ‘the weaponisation of visibility’. Through screenshots, hashtags, and going viral, the subject is turned into a spectacle of condemnation in the public domain on the basis of religion, nationalism or the honour of the family. Stanley Cohen's theory of moral panic explains the intensity of these episodes: communities tend to overreact disproportionately to perceived threats to dominant values, and this overreaction is amplified when mediated through platforms optimised for emotional engagement¹⁸. Because public accusation alone often functions as a finding of guilt, digital vigilantism and it dispenses with the procedural protections- notice, evidence, and the opportunity to respond which distinguish formal justice from mob punishment.

Technology, Anonymity and Moral Policing in Digital Spaces: Technology plays an important role in this process of digital moral policing as well. Social media algorithms usually draw people's attention to emotionally loaded content since emotions drive attention and interaction¹⁹. In turn, offensive posts and campaigns could travel faster through social media than complicated topics and explanations of those topics. Safiya Umoja Noble states that digital technologies are not value-free instruments, but they are structures informed by social and political disparities. Thus, social media platforms perpetuate and escalate societal prejudices concerning gender, ethnicity, religious beliefs, and sexuality.

Lastly, anonymity has turned out to be an essential element that impacts the severity of moral policing on the digital platform. People can become involved in cyber harassment programs and still keep their identity since social media platforms are anonymous, and it makes people act aggressively when they do not have to act in the same way in real life. As stated by Danielle Keats Citron, cyber harassment thrives in an environment where people can commit their offences without being held accountable for it.

¹⁸ Stanley Cohen, *Folk Devils and Moral Panics* (1st edn, Routledge Classics 2011)

¹⁹ Greg Stratton et al., 'Crime and Justice in Digital Society: Towards a 'Digital Criminology'' (2017) 6(2) International Journal for Crime, Justice and Social Democracy

<https://www.researchgate.net/publication/317274183_Crime_and_Justice_in_Digital_Society_Towards_a_'Digital_Criminology'> accessed 12 June 2026

Yet another key issue associated with digital moral policing lies in the way social media itself has turned into a type of “public courtroom.” Contrary to legal proceedings, which involve proper evidence and follow certain legal procedures, online punishment tends to be quick and emotional without being subject to any regulations. Public outrage often replaces proper procedures, while the use of algorithms helps to increase visibility without differentiating between fair criticisms and harassment. In this regard, Tarleton Gillespie suggests that platform governance has gained an essential role in governing public discourse and regulation.

In fact, the case of digital moral policing is another example demonstrating how online environments can serve as means of informal justice and social control. Indeed, through the use of surveillance, public shaming, and algorithms that amplify the reach of information, social media allows users to collectively enforce their dominant norms and punish others for deviance from such norms. Thus, it becomes evident that rather than mirroring existing inequalities, digital environments tend to intensify and reproduce them.

CONSTITUTIONAL AND LEGAL CHALLENGES

India's constitutional and statutory framework offers real, but incomplete protection against digital moral policing. If examined closely, it can be noted that each instrument in this framework was designed with a different problem in mind, and each therefore struggles to address the coordinated, anonymous, and rapidly escalating character of online harassment. Article 19(1)(a) of the Constitution guarantees freedom of speech and expression, a right the Supreme Court has extended to online communication as a vital medium of democratic participation²⁰. This right is not absolute: Article 19(2) permits reasonable restrictions in the interests of public order, decency, morality, and defamation, among other grounds²¹. The difficulty is definitional rather than doctrinal; courts have not settled any form of test for distinguishing legitimate, if harsh, criticisms from a coordinated campaign of intimidation, and how the same constitutional provision protects the victim's critics and her harassers at the same time.

Challenges with the Constitutional Framework: The scope of the meaning of Article 21's guarantee of life and personal liberty has been expanded to include dignity, autonomy,

²⁰ Constitution of India 1950, art 19(1)(a); *Shreya Singhal v Union of India* (2015) 5 SCC 1

²¹ Constitution of India 1950, art 19(2)

reputation, and privacy, each of which is placed directly at risk by online shaming²². Yet Article 21 operates classically as a shield against state action; its application to harm inflicted by decentralised, private, and often anonymous online actors remains doctrinally underdeveloped, leaving victims with a constitutional interest but no clear constitutional remedy against non-state harassers. In *Shreya Singhal v Union of India*, the Supreme Court struck down section 66A of the IT Act as unconstitutional and vague, holding that criminalising “annoying” or “inconvenient” online speech violated Article 19(1)(a). This judgment was an important protection from arbitrary censorship; the effect of this decision is the abrogation of the only law from the IT Act that prohibited offensive communications.

In *Justice K.S. Puttaswamy v Union of India*, a nine-judge bench recognised privacy as a fundamental right under Article 21. This ruling is directly relevant to digital moral policing, since doxxing, non-consensual circulation of images, and reputational attacks all implicate informational privacy²³. While the Puttaswamy case creates a right vis-à-vis the State, the same cannot be said about any remedy that can be enforced against private individuals whose identity is anonymous.

Limits of Existing Statutes: The main law dealing with digital offences in India is the Information Technology Act 2000 (“IT Act”). The Act contains provisions related to cybercrime, breach of privacy, obscenity, and communication-related offences. Some sections of the IT Act can be applicable when dealing with digital moral policing and cyber stalking offences.

Important sections include:

- Section 66E - Punishment for violation of privacy.
- Section 67 - Punishment for publishing or transmitting obscene material electronically.
- Section 67A - Punishment for sexually explicit electronic content.
- Section 72 - Breach of confidentiality and privacy.

These provisions may apply in situations involving non-consensual circulation of private images, cyberstalking, or online abuse. However, the IT Act was enacted before the rise of modern social

²² *Shreya Singhal v Union of India* (2015) 5 SCC 1 (SC)

²³ *Justice K S Puttaswamy (Retd) & Anr v Union of India & Ors* (2017) 10 SCC 1 (SC)

media culture and therefore struggles to adequately address large-scale online harassment and coordinated digital vigilantism.

The next essential element of cyber regulation involves intermediary liability. Sites such as Meta, Google, and X (formerly Twitter) act as intermediaries since they serve as the means through which users share their content on the internet. Intermediaries are exempted from liability for any third party's content as long as they exercise due care and follow relevant laws, according to section 79 of the IT Act²⁴. In addition, under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, intermediaries must remove content that is unlawful²⁵.

Nevertheless, there is no consistency in ensuring that these regulations are adhered to. This is because harmful content continues to circulate very quickly before being acted upon by the intermediary. In addition, it takes a lot of time for victims to have their cases reviewed and have their complaints of harassment handled.

In spite of the constitutional rights and cyber laws, formal legal frameworks face many challenges in handling digital moral policing. One key limitation includes anonymity. Online users can create fake or anonymous profiles, making it difficult to trace the perpetrators and prosecute them. Digital moral policing campaigns are likely to involve many people acting in unison, thereby diluting the process of legal accountability.

Another limitation is jurisdiction issues. Online activities transcend international boundaries. The abusive material might emanate from another state or even another country, and evidence can easily be erased or modified. Moreover, the police might lack the necessary technological skills and resources for conducting online investigations.

A third limitation includes the speediness of online communications. While the outrage spreads quickly via reposting, tagging, screen grabbing, and algorithms, legal actions take time to go through due process. By the time the police make their move, the damage will have been done. Danielle Keats Citron argues that cyber harassment thrives in the current legal system because it is poorly suited to counteract the magnitude and speed of online abuse.

²⁴ Information Technology Act 2000, ss 66E, 67, 67A and 72

²⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

Social attitudes challenge legal protection in that they inform the way society reacts to digital moral policing. Victims, especially women, are likely to be subjected to discourses that blame them for being victims of harassment, discouraging them from pursuing legal action against their harassers. Furthermore, digital harassment may be viewed as ‘online drama’ or simply an unavoidable aspect of online life. Hence, legal action does not suffice in addressing the underlying social and cultural issues.

These problems with the legal approach highlight a much bigger problem: digital moral policing does not just exist as legal offenses but also as social acts informed by patriarchal society, cultural attitudes, and technology. The need for legal frameworks such as constitutional rights and cyber laws should not be discounted; however, they are inadequate on their own to counter the present acts of digital vigilantism, moral policing, media trials, etc.

CASE STUDY: ONLINE HARASSMENT OF FEMALE JOURNALISTS IN INDIA

The cyberbullying of women journalists in India is one of the best examples of how digital moral policing takes place using the tools of misogyny, intimidation, and nationalism. Female journalists who raise their voice regarding politics or criticism of hegemonic discourse of society are often subject to online bullying, rape threats, insults, and character assassination.²⁶ This kind of harassment is indicative of broader patriarchal attempts to control women’s participation in public discourse and to intimidate dissident voices through intimidation and humiliation.

Many notable journalists, such as Rana Ayyub and Barkha Dutt, have faced persistent cyber harassment. Rana Ayyub, a well-known investigative journalist who criticises majoritarian politics in India, has faced death threats and rape threats on the internet and has been the victim of disinformation campaigns. Sometimes, even morphed images and disinformation were circulated to intimidate her and keep her quiet. Similarly, Barkha Dutt, a respected journalist, has faced constant misogynistic remarks and been accused of being a bad nationalist.

Female journalists are typically harassed due to a mixture of misogyny as well as political and cultural policing. Those women who stand against dominant ideologies are referred to as “anti-nationals,” “immoral,” or “traitors.” As a result, cyberspace becomes an arena where digital vigilantism takes place. Such types of harassment do not imply just disagreement and criticism

²⁶ *The Chilling: Global Trends in Online Violence Against Women Journalists* (UNESCO, 2021)

but also shaming and silencing women from the discussion process. As pointed out by Danielle Keats Citron, cyber harassment usually implies attempts to undermine the credibility of women by making threats and defamation.

This is another instance of how inadequate our present-day law is for handling abuse in cyberspace. While it is true that there are certain constitutional laws as well as cyber laws, their implementation is not only slow but also inefficient. The availability of anonymous profiles, rapid dissemination of abusive content, and the non-accountability of the platforms have made it impossible to curb the abuse.

From a sociological perspective, the phenomenon of cyberbullying of female journalists is an instance of a bigger pattern of patriarchal surveillance and informal social control. Utilising technology makes it possible for the online community to impose collective discipline on those women who have appropriated public spaces and challenged gender norms. Thus, cyberbullying in this context is an instance of informal justice wherein the members of social media platforms enforce ideological conformity by means of intimidation and stigmatisation.

CONCLUSION

In the context of this article, digital moral policing can be described as the process of informal justice, which is built on the decentralisation principle of surveillance and punishment using the methods of trolling, shaming, doxxing, and vigilantism by upholding the cultural/patriarchal hierarchy tradition via the use of modern technology. Using perspectives of Foucault's theory about disciplinary power, Goffman's theory on stigma, as well as the concepts and ideas of feminist jurisprudence offered by Butler and MacKinnon, it can be deduced that digital moral policing is not an incident of cruelty but a form of control used against particular individuals who violate the accepted norms.

Keeping this in mind, the constitutional and legislative protections that exist in India under Articles 19(1)(a) and 21, landmark judgments such as *Shreya Singhal* and *Puttaswamy*, the Information Technology Act 2000, Intermediary Guidelines and Digital Media Ethics Code Rules 2021, and the Digital Personal Data Protection Act 2023 prove to be insufficient despite being necessary. The primary issue with their effectiveness is that they have been framed based

on the context of a real act of wrongdoing perpetrated by an individual against some duties towards the state, but digital moral policing is both anonymous and private.

It follows that addressing the problem of digital moral policing requires much more than changes within the judicial system. What is needed is enforcement of clear deadlines for takedown of organised harassment and non-consensual content from the platform rather than mere adherence to the standards that the law permits. It requires an ability and process of investigating anonymous and international harassment campaigns at the same speed as online virality happens, while keeping in mind, at the same time, the constitutional guarantees of rights of Article 19 and 21. And what is required of the Indian data protection regime is that it should be developed such that it provides those who are victims of doxxing and image-based sexual abuse an easy way of recourse, which is effective and viable at the same time.

However, on the surface of it, it appears that no matter how many reforms there are to the existing laws, they would never replace or change the very social understanding of online shaming as everyday talk rather than harm. The challenge for social media, lawmakers, and courts trying to govern digital public space is going to remain one of building institutions capable of addressing the harm which is collective in its origin yet personal in its impact.