



Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India

Debarati Halder & Subhajit Basu

To cite this article: Debarati Halder & Subhajit Basu (30 Sep 2024): Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India, Information & Communications Technology Law, DOI: [10.1080/13600834.2024.2408914](https://doi.org/10.1080/13600834.2024.2408914)

To link to this article: <https://doi.org/10.1080/13600834.2024.2408914>



© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 30 Sep 2024.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India

Debarati Halder^a and Subhajt Basu^b

^aParul Institute of Law, Parul University, Vadodara, India; ^bSchool of Law, University of Leeds, Leeds, UK

ABSTRACT


This article provides a critical analysis of the complex nature of non-consensual image-based harassment of women in cyberspace, challenging the prevailing view that this form of harassment is synonymous with revenge pornography. It explores the intricate patterns and methods through which images are used to target women online, with a specific focus on the Indian context. The article has three primary objectives: firstly, to delineate and comprehend the diverse patterns of this digital abuse and its repercussions on the victimisation of Indian women; secondly, to investigate the root causes and consequences of such victimisation within India; and thirdly, to propose policy measures, especially through civil and criminal remedies, aimed at curbing the production and dissemination of this detrimental content. Providing critical insight into the problematic relationship between content creators and websites, which is intensified by jurisdictional boundaries imposed by foreign laws that govern these platforms, the article argues that this legal incongruity may inadvertently allow content creators to persist in their harmful practices despite the legal protections currently available in India. Consequently, it calls for a reassessment of existing legal frameworks and argues for the development of stronger, more cohesive global policies to address this issue effectively.

KEYWORDS

Nonconsensual image-based harassment; website liability; legal remedy; revenge porn; voyeurism; sextortion; cyber-crimes against women India

1. Introduction

The expert group report from the 67th session of the United Nations Commission on the Status of Women highlighted a significant contradiction in the digital era. Although technology has empowered women globally, it also opens up avenues for victimisation, particularly through non-consensual image-based harassment.¹ This dichotomy is especially pronounced in India, where the internet user base has expanded to over 759 million, 57%

CONTACT Subhajt Basu  s.basu@leeds.ac.uk

¹Expert Group Meeting Report: Innovation and Technological Change, and Education in the Digital Age for Achieving Gender Equality and the Empowerment of All Women and Girls' <https://www.unwomen.org/sites/default/files/2023-02/CSW67-Expert-Group-Meeting-report-en.pdf> accessed 23 January 2024.

© 2024 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

of whom are women.² In response to the urgent need for legal measures to combat online crimes against women, the Indian Parliament has introduced several key pieces of legislation. These include the *Information Technology Act 2000* (amended in 2008), the *Protection of Women from Sexual Harassment at Workplace Act 2012*, the *Protection of Children from Sexual Offences Act 2012*, and the *Digital Personal Data Protection Act 2023*. Additionally, the *Indecent Representation of Women (Prohibition) Act 1986* was amended in 2018 to extend its scope to the digital realm, specifically targeting the indecent representation of women online.

This paper examines non-consensual image-based harassment in India, a country grappling with the complexities of digital crimes against women amidst its socio-legal development. Despite progress made through the *Information Technology Act 2000* and its subsequent amendments, a significant gap remains in addressing the full spectrum of non-consensual image-based offences. These crimes go beyond traditional categories such as revenge pornography, voyeurism, and sextortion, demanding a more comprehensive legal and societal response. India's context represents a unique intersection of technological advancement and deeply ingrained patriarchal norms. This paper aims to explore this intersection, presenting four case studies that illustrate the multifaceted nature of the digital victimisation of women in India. These incidents have repercussions as personal tragedies and societal failings within the country's socio-cultural framework. The case studies discussed are: the *Ritu Kohli* case, considered India's first reported instance of online harassment; the *Rana Ayub* case, where deepfake technology was misused to clone her identity for harassment; the *Sulli Deals and Bulli Bai* cases, where images of female journalists were uploaded onto digital platforms as 'auction items' for virtual sexual exploitation; and the *Rashmika Mandana* case, in which a deepfake video of the actor was widely circulated on social media.

The 2012 Delhi gang rape case highlighted critical flaws in the existing legal framework, revealing its inadequacy in addressing various forms of online harassment and exploitation targeting women. This tragedy led to the enactment of the *Criminal Law Amendment Act 2013*, which introduced provisions to the *Indian Penal Code*³ against sexual assault, voyeurism, cyberstalking, and other forms of online harassment. While these amendments represented a significant shift in legislation, focusing primarily on sexual offences, they did not fully encompass the wide range of non-consensual image-based harassment.

For an extended period, researchers, government stakeholders, and non-governmental organisations have been clarifying the concept of online gender-based harassment. Initially defined as crimes using modern telecommunication networks such as the internet (including chat rooms, emails, notice boards, and groups) and mobile phones (SMS/MMS), the scope of these crimes has significantly broadened. The expanded terminology now includes various forms of online crimes against women, such as online misogynist speech, trolling, gender bullying, online grooming, privacy infringements (including hacking), revenge pornography, non-consensual cyber pornography, voyeurism,

²PTI, 'Over 50% Indians Are Active Internet Users Now; Base to Reach 900 Million by 2025: Report' *The Hindu* (4 May 2023) <https://www.thehindu.com/news/national/over-50-indians-are-active-internet-users-now-base-to-reach-900-million-by-2025-report/article66809522.ece> accessed 23 January 2023.

³Indian Penal Code 1860 was replaced by Bharatiya Nyaya Sanhita ('Indian Justice Code') on December 25, 2023.

sexting, and cyber obscenity.⁴ The term 'online gender-based violence' has been widely adopted to encapsulate these phenomena.

Recent studies have further developed our understanding of victim types, categories of harassing behaviour, and potential solutions.⁵ This includes identifying six types of technology-facilitated gender-based violence: harassment, image-based sexual abuse, non-consensual distribution of intimate images, voyeurism, sexual exploitation, sextortion, doxing, and documenting or broadcasting sexual assault.⁶ Platforms like Twitter (now X) are commonly used for technology-facilitated gender violence, often involving offensive language and primarily focusing on text-based harassment.⁷ In their research on online violence against women journalists, Posetti et al. noted that the most common patterns of online harassment include misogynist abuse and threats, using racial slurs against victims, privacy infringement, and sharing disinformation.⁸ Additionally, the emergence of deepfakes has been recognised as a growing trend in online harassment, especially targeting female journalists, activists, and celebrities.⁹ Hence, the prevailing focus on image-based online gender harassment, particularly involving sexually abusive content, points to several critical implications and needs in the field of online safety. This focus underscores the urgent requirement for enhanced legal frameworks and enforcement mechanisms that can effectively address and deter such forms of harassment. We argue that existing laws do not fully capture the nuances of image-based abuse or provide adequate protection against emerging technologies like deepfakes, which can be used maliciously.

As previously discussed, Indian legislation, including the *Criminal Law Amendment Act 2013* and the *Information Technology Act 2000* (amended in 2008), recognises offences such as cyberstalking, voyeurism, non-consensual sharing of pornography, capturing rape videos, and disseminating such material. However, both governmental and academic research has not adequately addressed several other forms of image-based harassment targeting women.¹⁰ While the classification of image-based sexual abuse covers various forms, including those related to revenge pornography, we argue that it does not fully capture the broader concept of non-consensual image-based online harassment. Discussions often focus on non-consensual pornography websites, noting the severe harm caused to individuals whose images are posted without consent, particularly the risks to reputation and personal security due to the potential inclusion of personally identifiable information.

⁴D Halder and K Jaishankar, *Cyber Crimes Against Women in India* (SAGE Publications, 2016).

⁵E Kavanagh and L Brown, 'Towards a Research Agenda for Examining Online Gender-Based Violence Against Women Academics' (2020) 44 *Journal of Further and Higher Education* 1379. Also see N Suzor and others, 'Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online' (2019) 11(1) *Policy & Internet* 84.

⁶S Dunn, 'Technology-Facilitated Gender-Based Violence: An Overview' Centre for International Governance Innovation: Supporting a Safer Internet Paper (2020) https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1774&context=scholarly_works accessed 7 January 2024.

⁷H Purohit and others, 'Gender-Based Violence in 140 Characters or Fewer: A# BigData Case Study of Twitter' (2015) arXiv preprint arXiv:1503.02086 <https://arxiv.org/abs/1503.02086> accessed 23 January 2023.

⁸J Posetti and others, 'The Chilling: Global Trends in Online Violence against Women Journalists' (UNICEF 2021) https://www.researchgate.net/publication/352561848_The_Chilling_Global_trends_in_online_violence_against_women_journalists.pdf accessed 12 January 2024.

⁹A Flynn and others, 'Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging Form of Image-Based Sexual Abuse' (2022) 62 *British Journal of Criminology* 1341.

¹⁰S Maddocks, 'From Nonconsensual Pornography to Image-Based Sexual Abuse: Charting the Course of a Problem with Many Names' (2018) *Australian Feminist Studies* <https://doi.org/10.1080/08164649.2018.1542592>

It is crucial to recognise that such non-consensual image-based harassment can occur in any jurisdiction.¹¹ However, certain South Asian countries like Pakistan, Bangladesh, Afghanistan, and Sri Lanka face heightened challenges due to a combination of factors. These include issues in skill-based job sectors, the allure of lucrative earnings from social media platforms through content creation and circulation, legal gaps, and a lack of awareness about image-based privacy and online gender-based violence.¹² This situation is particularly significant as these countries, like India, share a common legal heritage rooted in patriarchal norms, owing to their historical connection with British colonial laws.¹³

Schoenebeck et al. examine various forms of online harassment on social media platforms, focusing on the harms caused by the non-consensual publication of images and personal information.¹⁴ They propose several remedies for these harms, including removing content, issuing apologies, and banning those responsible for uploading the content.¹⁵ While we agree with their recommendations, we identify a gap in understanding regarding the practical implementation of these remedies – particularly whether responsibility should lie with social media companies and the perpetrators or be shared between platforms and offenders. This distinction is especially important when the perpetrator operates from a different jurisdiction or has fled to avoid legal consequences but still controls the data used in the harassment. In addressing remedies, Katz explores copyright law as a potential avenue to deliver justice for victims of non-consensual image-based harassment in cyberspace.¹⁶ This approach is echoed by several other researchers¹⁷, indicating a broader academic consensus on potential legal frameworks for addressing such harassment.

While existing studies¹⁸, have explored various patterns of image-based sexual abuse, including aspects of revenge porn; there is a noticeable lack of research on expanding the concept of non-consensual image-based victimisation beyond sexual abuse to include revenge porn. Nonconsensual image-based victimisation can manifest in several forms,

¹¹See C McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37(3) *Oxford Journal of Legal Studies* 534–561. See also N Henry, Asher Flynn, and Anastasia Powell, 'Policing Image-Based Sexual Abuse: Stakeholder Perspectives' (2018) 19(6) *Police Practice and Research* 565–581.

¹²N Sambasivan and others, "'They Don't Leave Us Alone Anywhere We Go': Gender and Digital Abuse in South Asia' in Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (2019) 1–14.

¹³See G Gangoli, 'Understanding Patriarchy, Past and Present: Critical Reflections on Gerda Lerner (1987), *The Creation of Patriarchy*, Oxford University Press' (2017) 1(1) *Journal of Gender-Based Violence* 127–134. See also Ellen Willis, 'Feminism, Moralism, and Pornography' in *Living with Contradictions* (Routledge, 2018) 161–164.

¹⁴S Schoenebeck, C Lampe, and P Triêu, 'Online Harassment: Assessing Harms and Remedies' (2023) 9 *Social Media+ Society* <https://doi.org/10.1177/20563051231157297>

¹⁵Ibid.

¹⁶R Katz, 'Takedowns and Trade-Offs: Can Copyright Law Assist Canadian Victims of Nonconsensual Intimate Image Distribution?' (2020) 29 *Education & Law Journal* 169 <https://www.proquest.com/openview/6bdea3a070efbd3b84316ff9fd720b98/1> accessed 12 February 2024.

¹⁷See M. A. Franks, 'Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators' (2015). Accessed 12 March 2024 <https://doi.org/10.2139/ssrn.2468823>; See also J. Beyens and E. Lievens, 'A Legal Perspective on the Nonconsensual Dissemination of Sexual Images: Identifying Strengths and Weaknesses of Legislation in the US, UK and Belgium' (2016) 47 *International Journal of Law, Crime and Justice* 31–43. <https://doi.org/10.1016/j.ijlcrj.2016.07.001>; T. Cole and D. Cole, 'Exploring the Effectiveness of Legislation Combating Digital Nonconsensual Sexually Explicit Image Distribution' (2022) *Journal of Victimology and Victim Justice* <https://doi.org/10.1177/25166069221117187>

¹⁸See M Yar and J Drew, 'Image-Based Abuse, Nonconsensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales' (2019) 13(2) *International Journal of Cyber Criminology* July – December 2019 [://efaidnbmnnnibpajpcgglefindmkaj/https://www.cybercrimejournal.com/pdf/YarDrewVol13Issue2IJCC2019.pdf](https://efaidnbmnnnibpajpcgglefindmkaj/https://www.cybercrimejournal.com/pdf/YarDrewVol13Issue2IJCC2019.pdf) ; See also M Aikenhead, 'Nonconsensual Disclosure of Intimate Images as a Crime of Gender-Based Violence' (2018) 30(1) *Canadian Journal of Women and the Law* 117 <https://doi.org/10.3138/cjwl.30.1.117>

such as creating mashed-up videos or collages using images of women from digital communication platforms. These creations, which may not necessarily be made for sexual gratification, often aim to generate viewer-based revenue. Such forms of non-consensual image-based victimisation remain under-researched in India, leading to a scarcity of data on the patterns of this type of victimisation and/or the reporting mechanisms in place. This paper attempts to bridge this gap by shedding light on these overlooked areas of nonconsensual image-based victimisation.¹⁹

This paper argues for an expanded legal interpretation and increased societal awareness of non-consensual offensive imagery. It contends that the existing legal framework and current societal discourse in India inadequately address the complex realities of these crimes. The paper underscores the necessity for a more comprehensive approach that aligns legal definitions and remedies, particularly through compensatory jurisprudence, with the complexities inherent in non-consensual image-based offences. The goal is to define the scope of non-consensual image-based harassment within the Indian context, uncover the motives behind capturing and disseminating such images, identify legislative and policy shortcomings, and propose a comprehensive legal overhaul. Furthermore, the paper emphasises the critical importance of digital literacy and empowerment in combating online gender-based violence, contributing a nuanced, scholarly perspective to the discussion on technology-enabled gender violence. It also argues that addressing non-consensual image-based harassment through legal mechanisms alone is insufficient. Social initiatives led by the government, schools, higher educational institutes, non-governmental organisations, and companies through corporate social responsibility programmes must also combat this phenomenon.

The paper is structured into six main sections, beginning with an introduction. The second section explores the patterns of non-consensual image-based victimisation, tracing developments from the Ritu Kohli case – India’s first reported instance of online harassment – to the Rashmika Mandanna incident. The third section examines and identifies patterns of non-consensual image-based victimisation, analysing why such content is inherently ‘offensive’ and not protected as free speech. It investigates various forms of image-based harassment, such as revenge pornography, sextortion, and voyeurism, arguing that these actions violate privacy and personal dignity. The fourth section addresses the impact of online victimisation on individuals and the lack of response from both the government and web companies. Victims often suffer severe psychological trauma, social ostracism, and career setbacks. The government’s response has been inadequate, and tech companies have not taken proactive measures to remove harmful content, leaving victims with insufficient recourse. The fifth section proposes a collaborative framework involving the government, private sector, and civil society to address non-consensual image-based harassment in India. This includes

¹⁹This research primarily focuses on identifying patterns of offensive, non-consensual images and the consequential victimisation of women in India. To address this issue, the authors examined relevant Indian laws to understand whether these laws categorise such harassment as offences and offer any form of justice restitution for the victims. Additionally, the study reviewed the reporting policies of three major social media platforms—YouTube, Facebook, and Instagram—to comprehend their policies regarding the takedown of offensive, non-consensual, image-based content targeting women. This analysis involved examining specific YouTube videos, some labelled as ‘controversial videos’ and others tagged with lines such as ‘papa ki pari’ and ‘funny wedding videos.’ The aim was to identify patterns by scrutinising the overall nature and intent behind creating and disseminating such content.

raising awareness, strengthening legal protections, and ensuring tech companies take responsibility for monitoring and removing offensive content. In the sixth section, the paper concludes by emphasising the importance of comprehensive legal reforms and international cooperation to tackle the global challenge of non-consensual image-based harassment effectively. The need for a unified policy approach, the empowerment of women to report abuse and a balanced legal framework are highlighted as crucial steps forward.

2. Patterns of nonconsensual image-based victimisation in India: case studies from Ritu Kohli to Rashmika Mandanna

In this section, we examine the patterns of non-consensual image-based victimisation, tracing their evolution from the landmark Ritu Kohli case to the more recent Rashmika Mandanna incident. By analysing these case studies, we gain a deeper understanding of the changing landscape of digital harassment in India. These examples provide valuable insights into how this issue has both persisted and evolved over time, highlighting the urgent need for updated legal frameworks and social awareness to address the growing complexities of online harassment.

2.1. Case studies

2.1.1. Ritu Kohli

Prior to the enactment of the Indian *Information Technology Act 2000*, which was primarily focused on e-commerce, there existed a significant gap in the legal infrastructure for recognising and addressing online harassment. Consequently, law enforcement was often ill-equipped with the understanding and tools necessary to support such crime victims adequately. This shortfall in legal preparedness became evident in the early 2000s, particularly with the Ritu Kohli case.²⁰ Kohli, among India's first women to fall prey to cybercrime, became a target in 2001 when one Manish Kathuria shared her phone number online after impersonating her on a chat platform, leading to an onslaught of unsolicited and explicit calls. Although Kohli's complaint was lodged under Section 509 of the Indian Penal Code, which penalises 'acts intended to insult the modesty of a woman,' this legal approach proved inadequate. It did not capture the complex nature of online harassment, which, in Kohli's case, involved impersonation and the misuse of personal information rather than simple 'cyberstalking.'

Kohli's experience exemplifies a broader trend of misunderstanding and mishandling online crimes against women, highlighting a disconnect between victims' actual experiences and the legal system's interpretation of such incidents. During this time, there were instances of law enforcement exhibiting insensitivity and a lack of awareness, occasionally attributing blame to the victims.²¹ This not only downplayed the severity of the offences but also deterred victims from seeking justice. Kohli's case, far from

²⁰S Kethineni, 'Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms' in K Jaishankar (ed), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (Palgrave Macmillan, 2020) 305.

²¹See Ravinder Barn and Ved Kumari, 'Understanding Complainant Credibility in Rape Appeals: A Case Study of High Court Judgments and Judges' Perspectives in India' (May 2015) 55(3) *The British Journal of Criminology* 435–453, <https://doi.org/10.1093/bjc/azu112>

being a mere instance of cyberstalking, represented a complex interplay of cyber impersonation and privacy violations. Unfortunately, this nuanced understanding was absent in the law enforcement and judicial responses at the time, culminating in the premature dismissal of her case without achieving proper redress.

2.1.2. Rana Ayub

The case of Rana Ayyub in 2018 epitomises the gaps in the legal response to sophisticated forms of digital identity harassment.²² Her ordeal with online predators, who manipulated her digital identity by creating cloned profiles and deepfake pornography, underscores the adaptability and malicious ingenuity of cyber harassers.²³ The sluggish and ineffective response of the Indian legal system, only rectified after significant international intervention, underscores a troubling gap between the evolving tactics of cybercriminals and the static nature of existing legal remedies. This disparity highlights the urgent need for a robust and adaptive legal framework to keep pace with the ever-changing cybercrime landscape. While foundational, the current legal framework must be continuously reassessed and revised to address the increasingly innovative and complex forms of digital harassment.

2.1.3. Sulli Deals and Bulli Bai

In 2022, a deeply disturbing incident occurred in India's digital space, where several Muslim women journalists faced egregious online harassment.²⁴ Their images were uploaded to GitHub, a Microsoft-based platform, with texts implying that these women were being auctioned. This act was not aimed at selling anything but at causing profound public humiliation. Unlike the impersonation Rana Ayyub experienced, these photos, sourced from various online platforms, were paired with demeaning and sexually explicit comments. The police responded by filing charges under Section 67 of the Information Technology Act, which deals with obscenity, along with provisions of the Indian Penal Code for spreading religious enmity and insulting women's modesty.²⁵ News reports indicate two cases were lodged, one in Delhi and the other in Mumbai. In both instances, the accused were granted bail, with courts citing the perpetrators' ages, their intent (*mens rea*), and their non-criminal family backgrounds as reasons. There is no indication from the reports that the courts advised counselling for the perpetrators or took measures to prevent them from posting further demeaning content about the victims or any other women.

While India's Information Technology Act 2000 prescribes penalties for creating sexually explicit material under Section 67A, it lacks specific mention of image morphing. Conversely, the Indian Penal Code includes a suite of laws under Section 354 series that address sexual harassment in both physical and virtual spaces. This encompasses

²²Ayyub R, 'I Was The Victim Of A Deepfake Porn Plot Intended To Silence Me' Huffpost (21 November 2018) https://www.huffpost.com/archive/in/entry/deepfake-porn_in_5c1201cfe4b0508b213746bd accessed 3 January 2024.

²³M. T. Pillai, *Affective Feminisms in Digital India: Intimate Rebels* (Routledge India, 2022).

²⁴N Thapliyal, 'Bulli Bai App Creation 'An Affront To Dignity Of Women Of Particular Community': Delhi Court Denies Bail To Neeraj Bishnoi' LiveLaw (14 January 2022) <https://www.livelaw.in/news-updates/delhi-court-denies-bail-to-neeraj-bishnoi-in-bulli-bai-case-189515> accessed 23 January 2023.

²⁵N Thapliyal (2022, January 14). Bulli Bai App Creation 'An Affront To Dignity Of Women Of Particular Community': Delhi Court Denies Bail To Neeraj Bishnoi. LiveLaw. Retrieved September 14 2024 from <https://www.livelaw.in/news-updates/delhi-court-denies-bail-to-neeraj-bishnoi-in-bulli-bai-case-189515>

sexual assault, disrobing of women, publishing such content online, voyeurism, stalking, online stalking, and any act or gesture that could insult a woman's modesty (Section 509 of the Indian Penal Code). However, this Code does not detail provisions for preventing and punishing the trafficking and misuse of images for widespread sexual harassment, revealing gaps in the legal framework against the entire spectrum of harassment.

2.1.4. Rashmika Mandana

On November 5, 2023, a deepfake video of Indian actress Rashmika Mandanna circulated across social media platforms.²⁶ The video was created by a fan who superimposed the actress's image onto footage of another female influencer, Zara Patel. This was done to increase viewership on his Rashmika Mandanna fan page, which struggled to attract attention. Almost a month later, police apprehended the creator of the deepfake. Although he was subjected to criminal proceedings, the video remained accessible on X (formerly known as Twitter). Links to the video continue to be active across various news channels, highlighting issues with content moderation and removing harmful material from social media platforms.

The above cases suggest different patterns of nonconsensual image-based victimisation of women in India and the ever-growing vulnerability of women in this regard. Moreover, a cursory search on YouTube for keywords like 'funny videos' or 'funny falls' reveals a troubling trend of content creation where personal images, including those of men, women, and children, are taken out of context and repurposed. These images, often harvested without consent from personal social media profiles or professional photographers' pages, are then used to create so-called humorous content. Initially intended for private sharing or commemorating special moments like weddings, these images, when manipulated, can cause considerable distress and embarrassment to the individuals featured.

Collectively, these instances underscore a critical and emerging challenge in India's cyber legal landscape. They highlight the intricacy of online harassment, extending beyond traditional forms of cyberstalking and impersonation to more nuanced abuses like character defamation and privacy invasion. These cases necessitate a stringent and responsive legal framework and call for an ethical re-evaluation of content creation and sharing in the digital sphere to protect individuals from such invasive and damaging exploitations. The 2008 amendment to the Information Technology Act 2000, although progressive in its attempt to encompass a broader range of cybercrimes, including impersonation, privacy violations, and cyber terrorism, unveiled the systemic inadequacies in addressing the nuanced complexities of digital harassment. The introduction of the 'body corporate' concept under S.43A was a commendable step in enhancing accountability for data protection. However, this legislative move, scrutinised through the lens of critical legal theory, reveals a partial approach towards the multifarious dimensions of cybercrimes.

This discourse explains the widespread dilemma of nonconsensual image-based victimisation, particularly targeting women within the digital domain. Within this sphere, breaches of privacy, augmented threats of harassment, and the potential for substantial

²⁶FP explainer, Rashmika Mandanna deepfake controversy: What are these AI-generated pictures, videos? Published in November 6, 2023 at <https://www.firstpost.com/explainers/what-is-a-deepfake-fraud-how-can-we-stay-safe-from-it-12882832.html> Accessed 10 January 2024.

damage to social esteem proliferate. The patriarchal societal structure of India amplifies the detriment experienced by women depicted derogatorily online, adversely affecting their standing in matrimonial and employment markets. Women portrayed as sexual commodities not only experience deep personal distress but also subject their families to societal shame and isolation.²⁷ Law enforcement agencies often downplay the seriousness of women's experiences with online harassment, making it more difficult for them to seek and obtain justice.²⁸ This minimisation, in turn, empowers offenders, heightening the victimisation of women both digitally and physically – a reflection of the broader societal context in India.

Hinson et al. (2018)²⁹ coined 'technology-based gender violence' to classify digital offences aimed at individuals predicated on sexual or gender identities. Although this terminology captures a range of cyber harassment forms, including revenge pornography and cyberstalking, it fails to encompass other detrimental nonconsensual image-based behaviours such as zoom-bombing, voyeurism, and impersonation. These manifestations remain insufficiently recognised and addressed by the academic community and the criminal justice system in India.

The prevailing legal framework primarily addresses offensive imagery in scenarios involving nudity, explicit content, and rape depictions, where the penalties typically result in bailable charges and nominal imprisonment durations. Many instances of image-based victimisation, such as revenge pornography, remain unaddressed due to cultural norms that dissuade women from speaking out. Victims may be unaware of the derogatory or satirical misuse of their images, a problem exacerbated by gender imbalances and a lack of empowerment in less urbanised and socio-economically marginalised regions of India.³⁰ While educated victims may seek recourse through social media's reporting mechanisms, these platforms often ignore such grievances if they do not align with their policy guidelines, allowing the indefinite online presence of such images. While legislative efforts to strengthen women's empowerment exist, changes in societal perceptions of gender bias have been incremental. Misogynistic mockery and impersonation cause significant distress to victims and their families. Women's social media accounts may face unwelcome scrutiny through demeaning texts, memes, and visuals, often culminating in harsh societal condemnation.

Furthermore, the moral policing of women's 'Westernised' portrayals fosters a hostile cyber environment.³¹ Although new regulations require intermediaries to identify and stop the redistribution of harmful content, actual implementation remains sparse. Victims need more than punitive actions against perpetrators; they deserve compensation for reputational harm, prompt deletion of objectionable content, and formal

²⁷T Saha and A Srivastava, 'Indian Women at Risk in the Cyber Space: A Conceptual Model of Reasons of Victimization' (2014) 8 *Int'l J Cyber Criminol* 57.

²⁸Danielle Keats Citron and Mary Anne Franks, 'Criminalizing Revenge Porn' (2014) 49 *Wake Forest L Rev* 345, U of Maryland Legal Studies Research Paper No 2014-1, available at <https://ssrn.com/abstract=2368946>.

²⁹L Hinson and others, 'Technology-Facilitated Gender-Based Violence: What Is It, and How Do We Measure It?' (International Center for Research on Women 2018) https://www.icrw.org/wp-content/uploads/2019/03/ICRW_TFGBVMarketing_Brief_v4_WebReady.pdf accessed 12 January 2024.

³⁰P Kumar, A Gruzd and P Mai, 'Mapping out Violence against Women of Influence on Twitter Using the Cyber-Lifestyle Routine Activity Theory' (2021) 65 *American Behavioral Scientist* 689–711.

³¹S Udupa, 'Gaalī Cultures: The Politics of Abusive Exchange on Social Media' (2018) 20 *New Media & Society* 1506–1522 <https://journals.sagepub.com/doi/pdf/10.1177/1461444817698776>.

recognition as victims. Ultimately, enhancing digital literacy and empowerment for women in India is crucial to mitigating online exploitation and violence.

3. Different patterns of non-consensual image-based victimisation

As the above discussion suggests, image-based online harassment of women necessarily includes offensive nonconsensual images; these are 'offensive' because such images are accessed, collected and distributed with criminal purposes mainly to cause harm to women victims. Nonconsensual image-based harassment in cyberspace includes sharing audio-visual and still images of individuals in cyberspace without the consent of the individual whose image is being shared. Such images may be captured by the perpetrator or any third party who may or may not have the legal authority to capture such images. Non-consensual images may be divided into the following categories:

3.1. *Revenge porn*

The nonconsensual image-based victimisation of women in cyberspace has received maximum attraction regarding the definition of the very term 'revenge porn'. United Nations Economic and social commission for West Asia (UNESCWA) has explained the term revenge porn from the perspective of nonconsensual pornography in the following words:

Nonconsensual pornography (the most common form of which is known as 'revenge porn') involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images. The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship, and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship. However, perpetrators are not necessarily partners or ex-partners and the motive is not always revenge.

The definition above primarily serves to delineate nonconsensual pornography, encompassing the concept of revenge pornography as well. Concurrently, it elucidates that non-consensual pornography does not invariably align with the definition of revenge porn. This distinction arises because, in some instances, nonconsensual pornography can be produced and disseminated absent the motive of revenge.³²

Revenge porn is essentially constituted with the image of the victim that does not carry consent or permission of the latter to be shared by the perpetrator. There may be different kinds of still or audio-visual images that may constitute revenge porn content: this may include a normal photograph or image of the victim in a compromising state with her intimate partner, which may or may not have been captured with the permission of the former, voyeur images that may have been captured by her intimate partner who may be her intimate partner or her workplace colleague or her relative. In some cases, it may be seen that while the image of the victim may have been captured with her permission, the image may not be stored in the devices of the perpetrator for private storing of memories purposes: the perpetrator may share the original image or doctored image which may or may not be accompanied with sexually explicit texts that

³²JS Sales and JA Magaldi, 'Deconstructing the Statutory Landscape of "Revenge Porn": An Evaluation of the Elements That Make an Effective Nonconsensual Pornography Statute' (2020) 57 Am Crim L Rev 1499.

may damage the reputation of the victim and the same may be done for the gratification of revenge. It is also considered to be wrong behaviour that causes distress.³³ It is necessarily a consequence of emotional hurt that may be caused due to a breakup between two heterosexual or homosexual partners or due to jealousy between workplace colleagues or two individuals who may be connected through family relations or social relations.³⁴

Women are often the primary victims of revenge pornography, but it would be incorrect to assume that men cannot also be victims. However, when considering the long-term effects of revenge pornography, women are generally seen as more vulnerable than their male counterparts. In the Indian societal context, revenge pornography can also lead to severe physical threats to women. Indian society is characterised by close-knit bonds with extended families and caste-based communities. If the emotional relationship between the woman and the perpetrator is exposed, her family may withdraw support to preserve the family's honour. This can subject the woman to harassment or, in extreme cases, the threat of honour killings. Additionally, she may be stereotyped within her community, losing opportunities for employment or marriage.

Unfortunately, Indian laws do not recognise revenge porn. There is a tendency in the criminal justice system in India to address any nonconsensual image-based harassment of women, including revenge porn through a bag of legal provisions including S.354C (addressing voyeurism), S.509 (addressing using word, gesture to harm the modesty of women), of the Indian Penal Code and S.67 (creation, distribution of sexually explicit contents), S.67A (creation, distribution of obscene contents in the cyberspace) of the Information Technology Act.

We argue that such treatment may fail to deliver justice, as the courts may not fully recognise the perpetrator's ultimate motive – revenge. As a result, the courts may not issue a restraining order preventing the perpetrator from using the victim's images or contacting the victim in the future. A notable example of this is the 2018 case from West Bengal, India, where a state public prosecutor successfully represented a woman who was victimised by revenge pornography created by a man with whom she had an emotional attachment.³⁵ Even though the accused received a five-year imprisonment sentence and the court ordered compensation for the victim, there is no information on whether the court took any steps to prevent the perpetrator from further using the victim's images.

3.2. Voyeur, non-revenge porn images

Women may be objectified through street photography. It is commonly observed that young adults and adolescents capture images, including 'upskirt' photos of women in public places, and upload these to cyberspace for unethical profit. Such photographs and audio-visual content are often taken in places like swimming pools, public bathing

³³Ministry of Justice, UK Government, 'Revenge Porn: Fact Sheet' (2015) <https://assets.publishing.service.gov.uk/media/5a80be45ed915d74e33fc281/revenge-porn-factsheet.pdf> accessed 9 February 2024.

³⁴S Bates, 'Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors' (2017) 12 *Feminist Criminology* 22–42.

³⁵S Brinda, 'Local Lawyer Wins Revenge Porn Case' *The Telegraph* (9 March 2018) <https://www.telegraphindia.com/west-bengal/local-lawyer-wins-revenge-porn-case/cid/1412240> accessed 12 February 2024.

areas, and sea beaches, where people are typically less clothed. Even though the owners of these venues (often private companies) may establish rules prohibiting photography in the bathing and changing areas, violations are frequent, occurring either through self-photography or the installation of hidden cameras.

Voyeuristic, non-revenge porn images may also be produced by unauthorised installation of hidden cameras in hotel rooms (especially those used by honeymoon couples) and public restrooms. The content captured in this manner may be sexually explicit, but it is not created for revenge. Instead, these images are uploaded to various social media platforms, including adult websites, for sexual gratification. While this content is not considered hardcore pornography, it often includes nonconsensual depictions of private parts and intimate activities of heterosexual or homosexual couples. Typically, this content is uploaded to attract like-minded subscribers seeking sexually gratifying material. Such content may also be used for sextortion.³⁶ Although Indian laws, such as Section 354C of the Indian Penal Code, address voyeurism, there are inadequate regulations for strict monitoring of social media platforms or mechanisms to identify such voyeuristic images unless they are reported.

3.3. Non-consensual-non voyeur images

Non-consensual, non-voyeur images are often captured by individuals who have no personal connection to the victim. These images may be taken in public places or at everyday social gatherings. Capturing images without consent, whether in public or private settings, invariably infringes on the privacy of the individuals involved. The widespread use of smartphones and other camera-enabled digital devices has made it easier to capture such non-consensual and non-voyeur images, particularly of women, which can lead to privacy violations. Adolescents and young adults frequently film random people, including women, to create content for videos and reels on social media. In doing so, they may capture images from angles that render the images sexually explicit or capture moments deemed highly amusing by viewers. The motivation for content creators is often the potential profit from social media companies, which may be based on the number of views and subscribers. The images captured in this manner are non-consensual and non-voyeur and typically do not incur the penal punishments associated with sharing non-consensual, sexually explicit content for sexual gratification or for unethical profit in cyberspace.

These images may also be accessed from third-party databases. This can occur when a perpetrator gains unauthorised access to a victim's social media profiles or private or government databases, including civil society members' photo images as part of sensitive personal data for e-governance. It is important to note that a third party's liability for capturing images may be authorised by law, especially in e-governance. For example, an image may be captured by CCTV installed for traffic police management if an individual violates a traffic rule or by cameras on private properties or dash-cams.³⁷ Since introducing the Information Technology Act in 2000 (amended in

³⁶M Senger, 'Couples at Hotel Room Secretly Filmed. 4 Arrested in Noida' *NDTV* (12 September 2023) <https://www.ndtv.com/cities/couples-at-hotel-rooms-secretly-filmed-4-arrested-in-noida-4300041> accessed 23 January 2023.

³⁷Consider the case of a viral video that was captured on a metro rail in India, which shows women fighting for seats on the train. This is available at [@https://youtube.com/shorts/E7LIHtYM-WA?si=1b8rVVErllgxVwI4](https://youtube.com/shorts/E7LIHtYM-WA?si=1b8rVVErllgxVwI4). A third

2008), India has developed an e-governance system that uses digital communication tools for effective governance. The concerned government departments are responsible for installing CCTV cameras and managing data, including images captured by these cameras.³⁸

Similarly, private companies may maintain facial impressions and CCTV footage of employees, customers, and beneficiaries who may be availing of the services of such companies. Indian Information Technology Act 2000(amended in 2008) mandates that all body corporates secure infrastructure to provide security to the data retrieved from the employees and beneficiaries. However, we have observed that on several occasions, a third party accessed CCTV camera footage or leaked it without authorisation. Consider the Delhi metro CCTV footage leak case in 2019: One of the CCTV cameras installed in the metro station captured intimate images of a couple. The clipping was shared on porn websites, and later it became a news item for many mainstream media companies. As a result, the clipping may still be found on the internet if keywords like 'Delhi Metro CCTV footage' or 'Delhi Metro viral video' are searched.³⁹ While some of such images may now be found with marbled facial images on YouTube or Instagram, clear facial or full-body images of women in awkward positions may also be found online, which may be used for creating mashed-up videos for unethical profit gain. It is pertinent to note that even though such sorts of nonconsensual image distribution may infringe on the privacy of women, neither there is no legal provision to prohibit and punish the perpetrator, nor are there many police reports in such cases in India.

Nonconsensual non-voyeur images and clippings may also be accessed from content shared by individual stakeholders involved in commissioned photography. These stakeholders may upload specific images and clippings of their clients on their business pages as samples of their work. However, these images are not free to use without the permission of the original creator, i.e. the photographer, and may also be protected by copyright belonging to the client. Nevertheless, perpetrators may download such content without authorisation and use it for mashed-up videos. A typical example of such content can be found under broad categories like 'Indian funny marriage videos' or 'funny falls videos.'⁴⁰ As discussed, there are no laws specifically prescribing punishment for such nonconsensual image distribution and resulting harassment, particularly targeting women. The Indian Copyright Act 1957 addresses nonconsensual image distribution to a limited extent, including deep fakes, particularly for photographs and video clippings produced by the parties themselves or commissioned photographers.⁴¹ The

party may have captured the images. Many share video clips that show identifiable images of women. Also, consider the video clippings showing women-driven two-wheeler accidents. Most of these are uploaded on YouTube as mashed-up videos of footage taken from private and CCTV cameras. Some of these videos are available @ <https://www.youtube.com/watch?v=NeV-d2kUdBQ>; <https://www.youtube.com/shorts/9aqq-kY1JvA> Accessed 12 December 2023.

³⁸N G La Vigne and others, *Evaluating the Use of Public Surveillance Cameras for Crime Control and Prevention* (US Department of Justice, Office of Community Oriented Policing Services, 2011) 1–152.

³⁹S Barman, 'Delhi Metro Orders Probe as Footage Featuring Couple is Leaked' *The Indian Express* (3 August 2019) available @ <https://indianexpress.com/article/cities/delhi/delhi-metro-orders-probe-as-footage-featuring-couple-is-leaked-5861920/> accessed 20 January 2024.

⁴⁰See, for example wedding videos that are uploaded by third party with tag lines such as funny videos, funny marriage videos @ <https://www.youtube.com/watch?v=OVCEsU-vJk4> ; <https://www.youtube.com/watch?v=u9mVLGAhvvg> accessed 14 September 2024.

⁴¹P Nema, 'Understanding Copyright Issues Entailing Deepfakes in India' (2021) 29 *International Journal of Law and Information Technology* 241–254.

image owner and the commissioned photographer may file a complaint with the website where their images/videos have been uploaded to create misleading, insulting comedy videos without permission. However, there is almost no reporting in this regard. Neither are the images considered stolen, misleading, or offensive nor are content creators prohibited from reusing such content without permission.

4. Impact of nonconsensual image-based victimisation on women

The profound trauma and long-term effects of non-consensual image-based victimisation on women cannot be overstated. As we have seen, these patterns of victimisation – whether through revenge porn, voyeuristic images, or other forms of non-consensual image use – subject women to severe psychological, social, and even physical consequences. In India, where societal pressures around family honour and community standing are significant, such victimisation can lead to ostracism, loss of employment or marriage prospects, and, in some extreme cases, physical threats, including honour killings. We have identified five significant impacts of non-consensual image-based victimisation on women in India, which highlight the multifaceted trauma that such acts can inflict.

4.1. Privacy infringement

Nonconsensual image-based harassment in cyberspace may result in different kinds of victimisation of women. Such victimisation may necessarily fall within the broader purview of privacy infringement. Nonconsensual images necessarily bear personally identifiable content, which may make the image easily recognisable. Social media companies are increasingly expanding the liability of the users by providing them with choices to share content with selected audiences. This means that users are now more responsible regarding their privacy choices. However, this in no way means that websites have shrunken their liabilities.⁴² As the above discussion may show, it is not always the victims who unknowingly allow their images to be shared by third parties on social media platforms. Nonconsensual images (especially non-voyeur-non-revenge porn images) may be illegally shared by third-party perpetrators infringing the privacy of the original data/image owners.

The traditional Indian concept of privacy, particularly concerning women victims, has been deeply influenced by the *Purdah* system.⁴³ This cultural practice has shaped the legal remedies available in India, especially within the Criminal Procedure Code of 1973, which initially allowed women to file complaints through male family members. This provision reinforced the patriarchal structure, making female victims dependent on male guardians for critical decisions regarding police engagement, formulation of charges against the accused, and pursuit of legal trials for justice.⁴⁴ Notably, before the

⁴²For understanding the policies of YouTube for privacy protection, harassment related policy, and take-down norms, see https://support.google.com/youtube/answer/2802268?hl=en&ref_topic=9282436; see for more about Facebook's privacy policy @ https://www.facebook.com/privacy/policy/?entry_point=facebook_page_footer; See for Facebook policy on bullying and harassment @ <https://transparency.fb.com/en-gb/policies/community-standards/bullying-harassment/> Accessed 14 September 2024.

⁴³S Basu, 'Policy-Making, Technology and Privacy in India' (2010) 6 *Indian Journal of Law & Technology* 65 <https://repository.nls.ac.in/ijlt/vol6/iss1/3> accessed 3 January 2024.

⁴⁴M Madan and M K Nalla, 'Sexual Harassment in Public Spaces: Examining Gender Differences in Perceived Seriousness and Victimisation' (2016) 26 *International Criminal Justice Review* 80–97 <https://doi.org/10.1177/1057567716639093>

introduction of the 2013 Criminal Law Amendment Act, women facing violations of bodily or image privacy lacked the opportunity to articulate the extent to which their personal privacy – as opposed to family honour – had been breached. The 2013 amendment introduced significant provisions under Sections 354, 354A, B, C, and D of the Indian Penal Code, emphasising the sexual victimisation of women and their independent right to seek justice. Although the Indian parliament has expanded women’s legal avenues to justice, remnants of the older system persist in the Criminal Procedure Code⁴⁵, permitting male family members to remain the ultimate arbiters of whether and how female victims in their families can pursue justice. This continued practice underscores the need for further reforms to empower women to access justice independently.

We argue that online victimisation by way of nonconsensual image sharing is not limited to the meaning of sexual victimisation alone. In cases of non-voyeur-non-sexual image-based harassment also, the victim may suffer privacy violations because the contents may tarnish her social reputation. Consider the cases of viral videos showcasing women drivers of two-wheelers committing accidents or women involved in ‘funny fall videos’, ‘funny wedding videos’: these may not have sexually explicit body images of the female victims, but still, they may violate the privacy of the victims as these videos may expose certain moments or emotions that the victims may not wish to share with the public. The victims may not find any legal remedy in criminal laws or the Information Technology Act, 2000 (amended in 2008) against the perpetrator or the website where the video/images may have been uploaded. The newly introduced Digital Personal Data Protection Act, 2023 (which mandates transparency in data processing) and The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 may offer some solace by directing the websites to remove the objectionable content. However, this may not be of any use, especially where the women victims may not be aware of where the images have been uploaded and how to approach the websites for serving a takedown notice.

4.2. Reputation damage

The dissemination of nonconsensual imagery can significantly tarnish the reputations of female victims,⁴⁶ a consequence deemed particularly severe in Southeast Asian contexts, including India, where societal structures are predominantly patriarchal. Consequently, the unauthorised distribution of images can inflict reputational harm on the individual victim and her familial unit. In such societies, the ramifications of reputational damage may adversely affect the marital prospects of the women involved or their female relatives. Additionally, victims may encounter detrimental effects within the employment sector, burdened with the sole responsibility of elucidating the circumstances surrounding the dissemination of sexually explicit photographs. Moreover, these individuals often bear the onus of demonstrating their innocence, necessitating the initiation of legal actions.

⁴⁵It was enacted in 1973 and came into force on 1 April 1974. On 26 December 2023, it was replaced with Bharatiya Nagarik Suraksha Sanhita (BNSS).

⁴⁶B Sciacca and others, ‘Nonconsensual Dissemination of Sexual Images among Adolescents: Associations with Depression and Self-Esteem’ (2023) 38 *Journal of Interpersonal Violence* 9438–9464 <https://doi.org/10.1177/08862605231165777>.

Consider the illustrative media account of a female academic from West Bengal, India, who became the subject of scrutiny following the circulation of her bikini-clad selfie on Instagram. According to reports, the controversy was ignited by a guardian's complaint after discovering his ward viewing the photograph. Notably, the academic uploaded the image as part of an Instagram 'story,' which automatically deletes after 24 hours, with disputes emerging after this duration. Reports indicate she claimed that the student accessed the image without her consent and knowledge of its presence on the platform.⁴⁷ This instance underscores the potential for victims of online nonconsensual image-based victimisation to experience both repeated and secondary victimisation.

4.3. Technology facilitated coercive control

Technology-facilitated coercive control (TFCC) has significantly increased in recent times, reflecting the growing role of technology in enabling such behaviours.⁴⁸ This includes vast ranges of digital coercive control mechanisms, including stalking, online abuses, and controlling the digital freedom and liberty of the victims. It may be seen that in the case of intimate partner victimisation cases, the perpetrator (who may have shared nonconsensual images) may try to control the victim by TFCC methods to stop the latter from accessing complaining authorities like the police, courts and even the intermediaries. This may result in creating perpetual trauma, self-harm and withdrawal symptoms in the victims. The TFCC method may also include sextortion. The term sextortion has received different definitions from different stakeholders. The International Association of Women Judges (IAWJ) have provided a brief definition of sextortion as 'abuse of power to obtain a sexual benefit or advantage.'⁴⁹

While this definition is very much associated with workplace sexual harassment, from the context of online sextortion, the definition has been broadened. Sextortion, therefore, may mean extortion of money by threatening to create large-scale reputation damage by sharing nonconsensual sexually explicit images and recorded sexually explicit voice and/or text-based communication of the victim with the perpetrator. We also opine that the TFCC method may include demanding ransomware by threatening to archive and share nonconsensual images.

4.4. Image trafficking

The dissemination of nonconsensual images, particularly leading to the creation and trafficking of deep fakes, represents a grave intrusion into personal privacy and autonomy, orchestrated through convincingly realistic simulations of videos, audio, images, and texts designed to deceive. These deepfakes often originate from the artificial intelligence-driven manipulation of images obtained without consent, highlighting a

⁴⁷G Pandey, 'Kolkata St Xavier's Teacher: "I Was Forced to Resign over Bikini Photos"' BBC (23 August 2022) <https://www.bbc.com/news/world-asia-india-62601044> accessed 20 January 2024.

⁴⁸Wendy O'Brien and Marie-Helen Maras, 'Technology-Facilitated Coercive Control: Response, Redress, Risk, and Reform' (2024) *International Review of Law, Computers & Technology* <https://doi.org/10.1080/13600869.2023.2295097>.

⁴⁹International Association of Women Judges, *Naming, Shaming, and Ending Sextortion* (2012) https://www.unodc.org/res/ji/import/guide/naming_shaming_ending_sextortion/naming_shaming_ending_sextortion.pdf accessed 12 January 2024.

burgeoning area of digital exploitation. Furthermore, image trafficking extends beyond the mere unauthorised use of an individual's likeness for creating content aimed at victimisation. It encompasses creating content that victimises identifiable individuals within such images and deceives third parties through the production of deepfakes, thus amplifying the reach and impact of the original violation.

Integral to the ecosystem of image trafficking for deep fakes is the phenomenon of data theft. In this context, data related to or embedded within images is appropriated, treating the images as sensitive personal data. This complex web of nonconsensual image distribution, data theft, and subsequent misuse in the form of hate crimes or other malicious intents underscores a critical challenge within digital spaces. The case of Bullibai in 2022 illustrates these issues. Despite the arrest of the perpetrators and the initial legal response by the government, the subsequent granting of bail to the accused raises significant concerns about the judicial system's grasp of online victimisation, particularly of women, and the pressing need for clear, enforceable laws addressing digital data privacy and the prohibition of non-consensual image distribution.

Women, as victims of nonconsensual image-based victimisation, occupy a position of unique vulnerability. This distinction distinguishes them from their male counterparts and underscores the need for specialised consideration and support.⁵⁰ Victims can be categorised based on their resilience, differentiating between universally vulnerable and uniquely vulnerable individuals – the latter being more susceptible to harm and its repercussions. This delineation provides a nuanced understanding that enriches the application of Martha A. Fineman's vulnerability theory.⁵¹ Fineman argues for recognising the universal vulnerability of all individuals and advocates for governmental intervention and support to safeguard people against these vulnerabilities. She asserts that the role of the state should extend beyond traditional notions of equality under the law and should instead aim to ensure substantive equality by providing targeted support and protection, particularly for those who are more vulnerable.

Building on Fineman's argument in the context of non-consensual image-based victimisation, it becomes evident that both the state and non-state actors have a critical responsibility to strengthen defences against such exploitation. This requires legal remedies and a comprehensive framework of support that addresses both the immediate and long-term impacts on victims. For women, who often experience compounded vulnerabilities due to societal, cultural, and gendered dynamics, the provision of such support is not merely a matter of redress but a fundamental requirement for justice and equity. The state's intervention, therefore, must be multifaceted, encompassing legal, psychological, and social support mechanisms that recognise and address the unique challenges faced by women in the digital age.

5. Collaborative approach for combating nonconsensual image-based victimization of women: government and private sector roles

Non-consensual image-based victimisation of women renders victims highly vulnerable to various forms of online and physical victimisation. While the government could

⁵⁰LS Perloff, 'Perceptions of Vulnerability to Victimisation' (1983) 39 *Journal of Social Issues* 41–61.

⁵¹Martha A Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition' (2008) 20 *Yale Journal of Law & Feminism* 1, 9–15.

implement protective measures by enacting laws to penalise such offences and restore justice for victims, the current legal framework in India presents significant shortcomings. Neither sextortion nor image trafficking for deepfake creation has been explicitly recognised in Indian law. Similarly, the concept of revenge pornography lacks distinct legal acknowledgement. This substantial gap has left female victims of non-consensual image-based victimisation as ‘guardianless victims’.⁵²

As previously discussed, legal scholars have proposed remedies from a copyright law perspective,⁵³ while others have advocated for the expansion of criminal laws to address non-consensual image-based victimisation of women explicitly. Although these suggestions are well-supported, achieving justice is not always feasible due to various technical factors, including the victim’s reluctance or her family members’ fear of public shaming. Building on this argument, we propose that the responsibilities of intermediaries and social media companies through which non-consensual images are disseminated or published should be significantly enhanced. Furthermore, laws regulating online crimes against women should be amended to reflect constitutional rights to privacy, restrictions on offensive speech that harms women’s modesty and decency, and the prevention of defamation. We suggest three specific remedial measures:

5.1. Strengthening the laws for monitoring the liabilities of intermediaries and data fiduciaries

Most social media companies hosted in the US prefer to apply US laws when defining and executing their liabilities towards subscribers/users. However, since 2008, Indian courts and the government have been exploring tailored responsibilities for these companies, particularly in controlling the depiction of sexual violence and child pornography. Under S.79 of the Information Technology Act 2000 (amended in 2008), intermediaries are exempt from publisher liabilities if they practice due diligence and address grievances regarding content and privacy violations. Despite these provisions, social media companies have often escaped liability for various reasons, including not recognising certain actions as offences under their policies or US laws.⁵⁴

In response, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, were introduced, expanding the scope of intermediary and social media company liabilities. Chapter II of these Rules mandates that intermediaries address offensive content as per Indian standards, particularly concerning nudity and hate speech. This approach aligns with UN guidelines, including those from the 67th Session of the Commission on the Status of Women, which focuses on tackling online violence against women and girls and promoting gender equality through digital education. However, the grievance redressal mechanism detailed in Chapter II of the Rules is not clearly reflected in government monitoring efforts.⁵⁵ The Rules lead back to S.79 of the

⁵²D Halder and A Saiyed, ‘Legal Challenges to Cryptocurrency and its Guardian-Less Victims in India: A Critical Victimological Analysis’ (2022) 60 *International Annals of Criminology* 79.

⁵³R Katz, ‘Takedowns and Trade-Offs: Can Copyright Law Assist Canadian Victims of Nonconsensual Intimate Image Distribution?’ (2020) 29(2) *Education & Law Journal* 169–190. <https://www.proquest.com/openview/6bdea3a070efbd3b84316ff9fd720b98/1?pq-origsite=gscholar&cbl=44752>

⁵⁴D Halder, *Cyber Victimology: Decoding Cyber Crime Victimisation* (Routledge, Taylor and Francis Group, 2021).

⁵⁵Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 has laid down three levels of self-regulatory mechanisms and oversight mechanism under Chapter II, III and IV. For more, see in Information

IT Act, which indicates that intermediaries may face third-party liabilities if they fail to follow due diligence. Notably, S.43A of the IT Act imposes penalties on corporations, including intermediaries, for negligence in protecting user data. This has been further addressed by the Digital Personal Data Protection Act, 2023, which establishes the Data Protection Board of India to monitor data fiduciaries' obligations⁵⁶, prescribing penalties up to two hundred fifty crore rupees for breaches.⁵⁷

Current laws addressing intermediary liabilities concerning due diligence and grievance redressal do not specifically cover the aiding, production, creation, or distribution of AI-generated deepfakes. This oversight remains embedded within broader due diligence obligations. We suggest that the Indian Parliament consider legislative amendments similar to the European Union's Artificial Intelligence Act, 2024, which not only identifies but also mandates action against offensive AI-generated content, such as deepfakes. However, the AI Act exempts certain AI-created content, such as parodies, which may be protected as free speech.⁵⁸ This is concerning as the Indian understanding of free speech, which often includes elements of defamation, indecency, and immorality, differs significantly from that in the US or UK. The proposed amendments could significantly impact legal liabilities under the Intermediary Guidelines and the *Information Technology Act 2000*(amended in 2008).

5.2. Proposed amendments in the Bharatiya Nyaya Sanhita for addressing non-consensual image-based victimisation and consequential reputation damage

It is important to recognise that non-consensual image-based victimisation can lead to reputation damage. In India, this issue is approached from two primary perspectives: (1) holistic character assassination through false allegations, including false criminal charges, and (2) indecent representation of women across various media. Indian defamation law is largely influenced by English laws, which shaped the framework for uniform criminal laws in India, including criminal defamation. However, unlike English laws, Indian statutes do not have specific provisions addressing slander and libel, considered forms of civil defamation in England.

Historically, Indian defamation was addressed under Section 499 of the Indian Penal Code (IPC), 1860, with the prescribed punishment outlined in Section 500 of the IPC. This entails a possible sentence of up to two years in simple imprisonment, a fine, or both. With the introduction of the Bharatiya Nyaya Sanhita in 2023, defamation and reputation damage are now addressed under Section 356.⁵⁹ In recent years, Indian judges

Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 available @ chrome-extension://efaidnbmnnnibpcjpcglclefindmkaj/<https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28up%20dated%2006.04.2023%29-.pdf>.

⁵⁶For more understanding, see Chapter 2 of the Digital Personal Data Protection Act, 2023 (Act No.22 and 2023).

⁵⁷See in Schedule in Digital Personal Data Protection Act, 2023 (Act No.22 and 2023).

⁵⁸Felipe Romero Moreno, 'Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content' (29 March 2024) International Review of Law, Computers & Technology <https://doi.org/10.1080/13600869.2024.2324540> accessed 12 February 2024.

⁵⁹This provision offers certain essential elements for defamation which include (a) spoken and/or written words about the victims which may represent false allegations, accusations that may be intended to read by others, (b) any signs and visual representation about the victim that may represent false allegations against the victim and (c) publishing of such false statements with an intention that such acts may necessarily cause harm to the reputation of victim. For more understanding, see in Bharatiya Nyaya Sanhita, 2023, Act no.45 of 2023. Available @ chrome-extension://

have taken the liberty to interpret writings and content as defamatory based on three main principles established in the case of *B.M. Thimmaiah vs. T.M. Rukmini* (2013).⁶⁰ These principles are: (a) the statement must be considered defamatory by right-minded individuals of fair intelligence, (b) the statement must be targeted at the victim, and (c) the statement must be published. In applying the first principle, Indian courts have relied on the English concept of innuendo, where the plaintiff bears the burden of proving the defamatory aspects of an ostensibly innocent statement. Notably, in the *B.M. Thimmaiah* case, the court followed the precedent set in *Cassidy vs. Daily Mirror Newspapers Ltd* (1929)⁶¹, establishing that the speaker's ignorance of the statement's potential consequences is irrelevant if the plaintiff perceives the statement as defamatory.

Existing Indian laws may offer various remedies for online sexual defamation that may represent the female victims as 'immoral'. In this regard, the Indecent Representation of Women (Prohibition) Act, 1986⁶² provides a better understanding of the reputation damage of women by way of indecent representation of the character of victim women. A plain reading of S.2 of this statute may suggest that the words 'indecent representation of women' skirt around the concept of indecent representation of the body shape and /or any part of her body that may '*deprave, corrupt or inure the public morals*'. While it may have the potential to address sexually explicit image-based harassment, such an explanation, however, may not accommodate the concept of non-consensual image distribution that may include harassment by AI-based image distribution, accidental falls, and normal photographs with offensive texts with sexual connotations. This statute does not offer satisfactory victim remedies as it puts more weight on punishment for the offender.

Although the above interpretations may seem appropriate for addressing non-consensual image-based harassment, where the content creator or publisher may be unaware of the impact on the victim's reputation, we contend that neither defamation laws nor the legal provisions addressing sexual harassment of women in India are sufficiently developed to address the complexities of non-consensual image-based harassment in cyberspace. Moreover, these laws fail to provide adequate remedies for victims. It is, however, important to acknowledge that certain forms of non-consensual image-based victimisation, including voyeurism, are covered under Section 357C of the Indian Penal Code (now Section 77 of the Bharatiya Nyaya Sanhita, 2023).

The Indian Penal Code, and now the Bharatiya Nyaya Sanhita, prescribe punishments for sexual offences, including voyeurism, stalking, and the non-consensual showing of pornography to women. In addition, some provincial governments have introduced victim compensation schemes, offering financial redress based on the severity of physical victimisation, mental trauma, and loss of employment opportunities. These schemes are

efaidnbmnnnibpcjpcglcfindmkaj/https://prsindia.org/files/bills_acts/bills_parliament/2023/The%20Bharatiya%20Nyaya%20Sanhita,%202023.pdf

The Nyaya Sanhita, 2023 under S.356 (2) also prescribes a punishment for defamation with jail term for a maximum period of two years or with fine or with both or with community services. S.356 (3) and (4) prescribes punishment of maximum 2 years of jail term with or without fine for intentionally, voluntarily and consciously printing, engraving and selling or offer to sale defamatory contents

⁶⁰See in *B.M Thimmaiah vs. T.M, Rukmini*, AIR 2013, Kar, 81.

⁶¹*Cassidy vs Daily Mirror Newspapers Ltd*, (1929)2 K.B.331

⁶²Act No.60 of 1986

funded by government victim compensation funds. However, such compensation is not available for other forms of victimisation, as discussed above.

The discussions suggest that India lacks a comprehensive legal framework to address the various forms of non-consensual image-based harassment of women and the associated remedies. Although existing laws cover some types of non-consensual image-based harassment, many other forms remain unaddressed. This legal deficiency hampers victims' ability to obtain adequate remedies, particularly in civil damages. The application of defamation laws, privacy laws, and laws governing the publication and distribution of sexually explicit content often fails to secure compensation for victims, even though offenders may face criminal punishment. Furthermore, offenders are not required to remove the offending content from digital platforms and search engines. As a result, even if an offender is arrested or fined, the possibility of harassing images reappearing online remains a significant concern.

To address this issue, we advocate for expanding defamation laws to encompass the publication of non-consensual images in cyberspace, along with a more precise legal definition of this offence. Strengthening the legal framework is essential to ensure victims receive appropriate restitution in such cases. Existing defamation laws do not provide sufficient civil remedies, and judicial decisions in India are often undermined by the destruction of evidence by both victims and perpetrators, poorly drafted charge sheets, and complications arising from foreign laws and jurisdictional issues. A uniform development of cyberpenology to address the non-consensual harassment of women could provide a more effective solution to these challenges.

The Bharatiya Nyay Sanhita, India's penal code, prescribes a maximum punishment of three years for first-time offenders of online stalking, voyeurism, and sexual harassment under Chapter V. The Sanhita prescribes an extended jail term of up to seven years for repeat offenders.⁶³ However, neither the Sanhita, the Information Technology Act, nor any other existing legal statutes provide a correctional system for perpetrators or specific procedures for delivering justice to victims apart from imprisonment.⁶⁴ We suggest broadening the scope of conflict of laws, including defamation laws, to incorporate civil remedies in cases of non-consensual image-based harassment of women. Additionally, we recommend the development of mechanisms to monitor the virtual behaviour of convicted perpetrators to prevent further victimisation through multiple anonymous handles and accounts.

The Indian criminal justice system, including the police, generally does not charge the accused offender or intermediary simultaneously. Typically, the intermediary becomes involved only after the accused has been identified and the police have registered a case. This procedural delay allows further circulation of offensive images, exacerbating the trauma experienced by victims. We propose that police officers receiving reports of such incidents should immediately inform the intermediary. Suppose the intermediary fails to restrict public access to the content within the stipulated 36-hour period as stated under Rule 3(d) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. In that case, the courts should also extend criminal

⁶³See chapter V of the Bharatiya Nyay Sanhita, 2023, Act No.45 of 2023.

⁶⁴Consider the deepfake video of Rashmika Mandanna, which is still available when this article was being written through different YouTube handles such as <https://www.youtube.com/watch?v=RozpsGzWLbE> with the title 'Rashmika Mandanna Hot Video Viral' || Deep Fake video went viral as Rashmika Mandanna || AI video'.

liability to the intermediaries, including the requirement to compensate for causing trauma and distress to the victims.

Consequently, we propose the introduction of a new legal provision specifically addressing non-consensual image-based victimisation and its remedy, which could be added to the Bharatiya Nyay Sanhita following Section 78, which prescribes punishment for stalking. This may be framed as follows:

S.78A. Nonconsensual image-based victimisation and remedies:

(i) Whoever creates, publishes, or circulates any image of women either through Artificial intelligence-based tools or images downloaded, distributed from CCTV camera footage without proper authorisation, images including facial images extracted, downloaded, retrieved from any website and online platforms without any proper authorisation and from any other data archive kept as a confidential data by any data fiduciary including that for biometric data used for government identity purposes including banking, health, court, educational, vehicle registration, licensing, passport and any other purpose for which biometric details including facial images may be required, for the purpose of having fun, causing defamation to the victim, for the purpose of uploading the same images on any website for entertainment and unethical profit gaining out of such uploading and distribution.

Commits the offence of non-consensual image-based victimisation, which is a nonbailable and cognisable offence.

(2) Any person who commits the offence mentioned in Subclause (1) shall be punished with imprisonment for a maximum period of three years for the first conviction and for five years for the second conviction.

(3) Any intermediary who fails to restrict public access to the same images within 24 hours after receiving reports either from the victim herself or from any public-spirited person shall also be liable under this Section and shall be liable to pay a fine of 20 lakhs, from which Rs.5 lakh must be paid as a compensation to the victim.

The victim of non-consensual image-based victimisation may be eligible for compensation of up to Rs. 5 lakhs for mental trauma and reputational damage, recoverable from the perpetrator under Section 357 of the Criminal Procedure Code, 1973. However, we strongly argue that such laws will not produce effective outcomes unless India advocates for a global treaty on the online safety of women and promotes mutual cooperation between nation-states to ensure the restitution of justice.

5.3. Creation of large-scale awareness about the publicly available tools provided by intermediaries to enhance user self-protection (especially for women)

The emergence of social media platforms such as Orkut, Myspace, and Facebook in 2004 made users increasingly aware of various reporting tools. These include the report menu, options to 'lock' albums and profiles to restrict access to unknown individuals, and mechanisms for submitting takedown requests.⁶⁵ However, passive websites like workplace

⁶⁵Ben Bradford, Florian Grisel, Tracey L. Meares, Emily Owens, Baron L. Pineda, Jacob Shapiro, Tom R. Tyler, and Danieli Evans Peterman. 2019. Report Of The Facebook Data Transparency Advisory Group. Technical Report. Yale Justice Col-laboratory, Yale Law School https://s21.q4cdn.com/399680738/files/doc_downloads/dtag_report_5.22.2019.pdf accessed 14 September 2024.

websites, professional sites, and web pages showcasing female employees, students, and clients may not offer protection against downloading or copying images. Perpetrators may download images from these sites and upload them to social media platforms with ulterior motives. In such cases, widespread awareness facilitated by social media companies about their newly developed tools and features can help victims and public-spirited stakeholders, such as schools, higher education institutes and NGOs, prevent the escalation of victimisation. For instance, many users may not be aware of the new tools and features developed by Meta, especially for Instagram, that protect against sextortion and intimate image-based abuses, released on 11 April 2024.⁶⁶ Furthermore, many researchers and experts in the field of free speech and online violence against women may also be unaware of the platforms of global expert bodies that significantly influence Meta's content regulation decisions.⁶⁷ All Meta users can access these platforms to appeal decisions not to act against specific content. Such awareness initiatives by intermediaries, individual stakeholders, NGOs, and educational institutions can help prevent victims from falling prey to hackers who demand high prices for removing unwanted content from social media platforms.

Despite concerted efforts, the issue of non-consensual image-based victimisation of women in India persists. A key factor contributing to this problem is the lack of empowerment among women in seeking justice. Another contributing factor is the absence of basic education and language barriers, as a significant proportion of the population in rural and semi-urban areas, including women and girls, may not be proficient in English. As a result, many individuals may not fully comprehend the impact of derogatory remarks, whether in English or any other Indian language. Moreover, they may lack the knowledge required to report such content to relevant websites.

As previously discussed, the patriarchal structure of society often prevents women from reporting victimisation to law enforcement agencies without the consent of male guardians. Although the government has introduced e-reporting platforms aimed at simplifying the process for many female victims of domestic violence and sexual offences, the accessibility of these platforms remains questionable for women from rural and semi-urban areas, as well as those from socio-economically disadvantaged backgrounds, who may have limited access to digital devices for personal use. Notably, the Government of India has launched an online platform accessible at cybercrime.gov.in; however, the effectiveness of such initiatives has not met expectations.

6. Conclusion

This article highlights the issue of non-consensual image distribution and the resulting victimisation of women. It discusses three broad patterns of non-consensual image-based victimisation, some of which are not currently recognised as offences in India. The article argues that without legal recognition of these patterns, the victimisation of women may escalate. Assigning responsibility to intermediaries and social media

⁶⁶See for more in New tools to help protect against sextortion and intimate image abuse (2024) Meta. <https://about.fb.com/news/2024/04/new-tools-to-help-protect-against-sextortion-and-intimate-image-abuse/> accessed 14 September 2024.

⁶⁷For example, the first author has used platforms like <https://oversightboard.com/> to share opinions about Meta's decision regarding content regulations.

companies to prevent the non-consensual distribution of images by users could be an effective mechanism to curb online victimisation. However, lawmakers must acknowledge these patterns of online victimisation and enact policies and laws to criminalise all such forms of non-consensual image distribution-based victimisation of women. Additionally, victimisation might be mitigated if women are empowered to report these crimes and pursue legal action for the restitution of justice. While removing the offending content is a primary demand of the victims, courts and lawmakers should also consider financial remedies to address reputation damage.

This article also contends that merely relegating perpetrators to the correctional administrative system may be insufficient to prevent such victimisation. Effective mechanisms should be established to define the responsibilities of the perpetrators, which may include government-monitored internet and digital device usage by the perpetrators, transferring the responsibility of content removal to them, including intermediaries, and ensuring direct compensation to the victims.

Furthermore, this article proposes amending the Bharatiya Nyay Sanhita to introduce a new provision to specifically address non-consensual image-based victimisation and its remedies. It also advocates for raising awareness about the tools offered by intermediaries for reporting offensive content, platforms for voicing concerns to influence tech companies' decision-making on online and offline safety, and government platforms for registering complaints about online harassment of women in India. Additionally, it suggests that governmental efforts should be directed towards creating multilateral treaties for cooperation in addressing online crimes against women. It is important to note that women in several South Asian countries face similar challenges concerning non-consensual image-based harassment. This article suggests that these countries could adopt the findings and recommendations presented here to address these challenges effectively.

Disclosure statement

No potential conflict of interest was reported by the author(s).