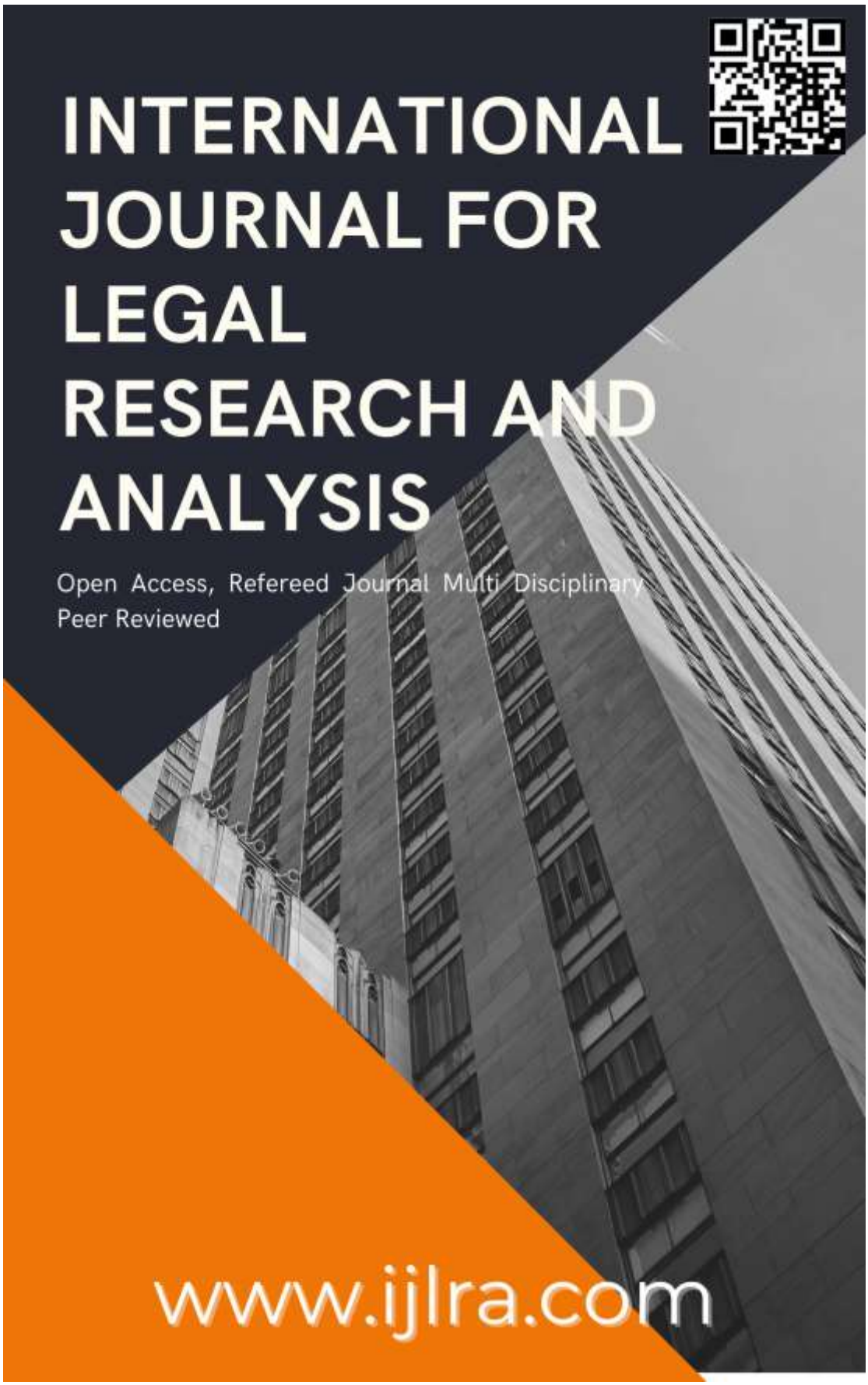

VOLUME 3 • ISSUE 8 • NOVEMBER 2026

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the International Journal for Legal Research & Analysis (IJLRA).

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ABOUT US

The International Journal for Legal Research & Analysis (IJLRA) (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the International Journal for Legal Research & Analysis aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The International Journal for Legal Research and Analysis (IJLRA) is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.

Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats.

The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published.

By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights.

The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

RESEARCH ARTICLE

From Non-Consensual Image Sharing To Algorithmic Abuse: A Critical Analysis Of Online Defamation And Cyberbullying In The Digital Age

Anamika • Sonali Pandey

Amity Law School, Noida
anamikaraj029@gmail.com
Amity Law School, Noida

ABSTRACT

The With the development of the digital public sphere came new ways of abusing people across the globe. Cyber-bullying and non-consensual image sharing have been well known issues of online abuse but with the development of new technologies, the modern abuse landscape has evolved. The abuse suffered by people on online platforms today is made easier and more effective through the tools available.

Non-consensual image sharing has become a major issue with the rise of synthetic media and deepfakes. This has highlighted the problems with the current legal framework defining the act. A victim of non-consensual image sharing cannot really pursue any legal action against an AI created image due to the uncertainty of where the synthetic asset falls in terms of jurisdiction. This is further exacerbated by recommendation algorithms which thrive off of creating content with a high level of arousal. This turns personal bullying into widespread defamation.

Ultimately, algorithmic abuse stems from the fact that platforms profit from engagement. Whilst social media platforms are often in the news for being poorly moderated and biased, the real issue is the neutral algorithms. Content is ranked based on the amount of engagement it receives meaning contentious and outrage causing content will be prioritized.

Any reactive approach to legislation will fail. In order to reduce abuse on online platforms, we must regulate the platforms themselves. Shifting the platforms to a safety by design model and revising tort laws will help reduce abuse on platforms.

Keywords: Algorithmic Abuse, Online Defamation, Cyberbullying, Non-Consensual Image

Sharing (NCII), Deepfakes and Synthetic Media, Platform Accountability, Algorithmic Amplification, Digital Permanence, Intermediary Liability, Safety by Design, Indian cyber law

1. INTODUCTION The growth of interactive web technology has created an environment where digital abuse is widespread. Cyberbullying between individuals has become more severe with the rise of “digital permanence” and the sharing of images without consent. Deepfakes and synthetic media have made things worse, with the potential to seriously damage reputations. It’s important to look at how cyberbullying has shifted from something between individuals to something fuelled by platforms, and how laws and policies can better protect people today. Modern defamation online is complicated. The attention economy and platform algorithms let individuals and groups spread extreme messages or coordinate abuse at massive scale. Existing laws and regulations are out of date and don’t offer enough protection to individuals. Because of this, platforms have too much power and users are exposed. In most cases, people are left to fend for themselves or file lawsuits. This paper will show how digital abuse has changed and what future research should investigate. It will also look at ways to improve online safety, especially by holding platforms accountable and revising tort liability laws.

1.1 Scope of Research This research aims to explore different sides of online digital violence. A main focus is on non-consensual image sharing, cyberbullying, and algorithmic abuse. The study also examines how deepfakes, AI-generated synthetic media, and digital permanence affect the privacy and reputation of people targeted by such acts. In terms of jurisdiction, the paper looks closely at Indian law, particularly the Information Technology Act (2000) and Bharatiya Nyaya Sanhita (2023). It also covers rules on intermediary liability and Constitutional rights under Articles 19 and 21. The analysis uses key court cases such as K.S. Puttaswamy v. Union of India, Shreya Singhal v. Union of India, and Mrs X v. Union of India.

1.2 Significance of the study This work draws attention to the move from individual, personal cyberbullying to collective abuse online, made possible by the attention economy. It shows that simply reacting to cyberbullying with new laws is not enough, especially since there is usually little focus on the needs of victims. Rather than sticking with victim-focused laws, there is a need to create

laws that address the business model of digital platforms. The recommendation is to include safety-by-design principles so that platforms are responsible for the way they organize and distribute content.

1.3 Research Methodology The methodology of this research follows a multidisciplinary approach. The research considers: • Legal issues: It reviews the shortcomings of current tort law, Indian statutes like the Information Technology Act and Bharatiya Nyaya Sanhita, and key judgments (including K.S. Puttaswamy v. Union of India) to highlight problems in the legal treatment of online defamation, cyberbullying, and algorithmic abuse. • Sociological issues: The study considers how the permanent nature of harmful online statements and images affects victims' mental health. • Technical issues: It explores the difficulties in auditing content recommendation algorithms and moderation tools, which sometimes unintentionally promote abusive material.

1.4 Research Objectives • Legal Frameworks: Critically examine the strengths and weaknesses of current Indian laws on cyber abuse, including the IT Act, Bharatiya Nyaya Sanhita (BNS), and tort law. • Platform Structures: Analyse how the business models and design of digital platforms, driven by recommendation algorithms and profit, can encourage cyber abuse and defamatory content. • Sociological Impact: Study the impact of permanent online content on the mental health of those affected. • Structural Recommendations: Suggest moving from reactive to proactive laws on digital abuse, including holding platforms accountable, updating tort law, and adopting safety by design.

2. CONCEPTUAL FRAMEWORK OF NON-CONSENSUAL IMAGE SHARING

2.1 Meaning and Nature of Non-Consensual Image Sharing

Non-consensual image sharing means distributing or posting pictures without the subject's permission. This often involves intimate or sexual photos or videos shared without consent. The phrase "revenge pornography" is often used for this type of abuse, especially when it's a partner sharing the images. However, there are many reasons someone might do this, including blackmail, harassment, humiliation, or trying to gain status. Intimate images can be shared on social media, messaging apps, forums, and more. Sometimes people share images with someone they trust, only to find out those images have been made public without their approval. Hackers may also steal private images. Giving permission to create or share media is not the same as giving permission to repost it elsewhere. If you haven't agreed to one, your rights to privacy and dignity may be violated, and there may be legal consequences. This kind of abuse may also come with threats, harassment, or false accusations. When images are widely shared and seen by many, it becomes a serious case of harassment and can damage someone's reputation.

2.2 Types of Image-Based Abuse: Leaked Images, Morphing and AI-Generated Deepfakes

There can be several types of image-based abuse:

• This involves sharing real personal images without consent: These may be photos taken privately or shared with a partner, but then distributed without permission. This is a breach of privacy and can have criminal or civil consequences. • Image morphing: Using editing software, a person's face can be placed onto someone else's body, or images can be altered to mislead. Sharing these manipulated images can cause embarrassment, harm reputations, and encourage harassment. • AI Deepfakes: Generative AI can now create convincing images or videos that show people in situations they were never in. When used to make non-consensual

personal images, this raises questions about consent, identity, privacy, and responsibility.1 • Threatening behavior: Victims may be threatened that their private images will be shared unless they pay money, do something, or give up control. If this behaviour meets the conditions for threats or extortion under the law, it can be a crime. • Resharing: Once images are out, they can be copied and spread again by others on new accounts or sites, leading to ongoing exposure and distress for the victim.

2.3 Consent, Privacy and Individual Dignity

Consent, privacy, and dignity are central to the issue of non-consensual image use. Consent means someone freely agrees to something. Privacy is about having control over personal matters. Dignity is about respecting a person's worth and not putting them in degrading situations.

In 2017, the Supreme Court of India recognized privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India. The judgment linked privacy to autonomy and dignity, making these constitutional principles key when considering digital rights violations. In the digital age, protecting privacy is complicated because personal data and images can be easily copied and shared widely.

If someone appears in a sexually explicit image that is later shared without consent, they are not at fault, even if they originally created or sent the image. The blame lies with whoever misuses and publishes the image. When images are posted with degrading captions or titles, the person's dignity is harmed. This kind of violation can lead to social stigma and even exclusion from workplaces or educational settings.

2.4 Distinction Between Image-Based Abuse, Online Trolling, Cyberbullying and Defamation

These terms are related but have different meanings : • Image based abuse means using images, especially intimate or sexual ones, abusively—such as by creating or sharing them without permission.

1 Okolie, Chidera. "Artificial intelligence-altered videos (deepfakes), image-based sexual abuse, and data privacy concerns." Journal of International Women's Studies 25.2 (2023).

• Online trolling is disruptive behaviour meant to provoke, ridicule, or create conflict in online spaces. Not all trolling breaks the law. • Cyberbullying describes targeted, ongoing bullying. It can involve threats, humiliation, harassment, sharing embarrassing material, or coordinated attacks. Definitions vary depending on the context.2 • Online Defamation is when someone publishes a statement that harms another's reputation. To count as defamation legally, the statement must meet certain requirements. Simply being rude or posting an embarrassing photo does not always qualify. The law looks at the content, its context, the people involved, available defences, and relevant legal standards.

A single incident might involve several different actions. For instance, if someone alters and shares a sexual image without permission, there could be multiple aspects: the act of publishing the image, others sharing it, and possibly false allegations being made. Posting the image can raise privacy issues, while making false accusations could lead to defamation claims. Being repeatedly targeted and harassed in this way may also qualify as cyberbullying.

This matters because different legal remedies might apply. If you pursue a privacy claim, your main goal might be to have the intimate material taken down. For a defamation claim, you would need to show that someone made a damaging statement about you. For criminal liability, you would have to look at exactly what the law requires.

ALGORITHMIC AMPLIFICATION AND THE SPREAD OF ONLINE ABUSE

3.1 Role of Social Media Algorithms and Recommendation Systems Social media sites use algorithms and recommendation systems to decide what content to show people. These systems might take into account how people interact with posts, how many times something has been viewed, how recent it is, how relevant it seems, and how likely you are to be interested. The details of how these algorithms work vary depending on the platform, and not all information is made public.

2 Ghosh, Ria, Meetu Malhotra, and Naresh Kumar. "Cyber bullying in the digital age: challenges, impact, and strategies for prevention." Combating cyberbullying with generative AI. IGI Global Scientific Publishing, 2025. 151-180.

Recommendation systems can let people see content even if they don’t follow the original poster. So, if you upload an image in a private group or small network, it might end up reaching many more people because it’s recommended, trending, found through a search, or shared more widely. While these systems can help users discover new information and connect with others, they can also cause problems. Harmful material that gains popularity may be pushed to a larger audience. A post that gets a lot of comments or shares may show up even more, depending on the platform. Still, it’s not accurate to say that every recommendation system is designed to promote abusive content. Sometimes content is spread because people share it directly, coordinate with others, or because of existing social networks. We have to look at what the algorithm actually does, based on the evidence. 3.2 Engagement-Driven Content Distribution and Viral Circulation Digital media often relies on metrics like likes, comments, shares, and views to identify and spread content quickly. This means both harmless and harmful content can go viral. Controversial or offensive posts can end up being shared by a lot of people. Non-consensual image sharing can spread widely because people are shocked, offended, or amused by the content. When that happens, the image might be shared along with new comments, or passed to other users through captions and replies. If a platform uses engagement as a sign of what’s relevant, then these reactions can help push the content far beyond its original group. However, many factors contribute to something going viral: user interaction, network effects, and media attention all play a role. It’s important not to assume that a post went viral only because of a platform’s recommendation system; it’s something that needs investigation. This shows that stopping online abuse is complicated, because individuals can help spread abusive content far outside its original audience. Images and videos can travel quickly, but not all cyberbullying cases start with a recommendation algorithm.

3.3 Algorithmic Amplification of Online Trolling and Harassment In Algorithmic amplification means that an automated system, such as a ranking or recommendation tool, pushes a piece of content to a wider audience. In cases where abuse has taken place, this can mean the harmful material is seen by more people—but whether this

actually happened needs to be shown in each case. For example, one person might post an explicit or doctored intimate image. Others then share it, sometimes adding comments or captions. The content can get further amplified if it attracts engagement or is recommended by the platform, exposing the victim to more harassment, insulting messages, and harm to their reputation. There can be many people involved in such cases. The person who posts the content is an abuser, but those who comment or share can also be part of the problem. Social media platforms that allow the content to stay up may also be implicated, although usually, they are seen as service providers. Online trolling often involves people piling on, trying to

pressure the victim into visiting certain sites or pages. Because so many people can be involved, it's hard for victims to take legal action against everyone. This swarm of activity can make it seem like there's a large organized group, even if most people involved only know a little about what's happening. Despite the numbers, it's important to think about what each person is doing. The original poster might be punished for sharing intimate material without consent. Those who comment or share might break the platform's rules. The platform itself usually isn't held legally responsible, since it's just hosting the service.

3.4 Role of AI, Image Morphing and Deepfake Technology Artificial intelligence has brought new challenges. Now, people can use generative tools to alter images and videos, creating misleading or fake material. This technology can be used to make non-consensual pornographic content or to make someone appear in a photo or video when they weren't actually present. This raises problems because it's hard to know who created the fake images or videos, how widely they have spread, and how many people have seen them. It's also difficult to verify whether material is authentic. Even if something is fake, it can still damage someone's reputation because people may believe it's real. These fakes are often used specifically to harm reputations, so these issues can't be ignored. In my view, the law should make clear distinctions between creating, publishing, and sharing such material. Punishments should be harsher for those who create the fakes than for those who merely publish or share them, although sometimes one person may do both. The creator

is the one most responsible for the harm caused. The Rashmika Mandanna deepfake incident that went viral in November 2023 is a good example of these problems. A deepfake porn video of the well-known model spread widely and even attracted positive attention before police intervened. This highlights the serious problems with deepfake pornography and why it should be treated as a crime. Still, it's best seen as a social issue rather than a legal precedent for future cases.3 3.5 Repeated Sharing, Digital Permanence and the Escalation of Harm These situations can have a long-lasting impact on victims. Once an image is out there, it can be downloaded, screenshotted, or copied by others. That means simply deleting the original post doesn't guarantee it's gone from the internet. Victims might keep receiving the image from others, directly or indirectly, and it could be seen by employers, schools, family, or anyone else. This creates practical problems for court-ordered takedowns. A judge might order the removal of a specific URL or user account, but it's impossible to know if every copy has been deleted. The image could still appear in search results or be re-uploaded by other users. The Delhi High Court, in Mrs. X v. Union of India (2023), looked at the ongoing circulation of non-consensual intimate images and the difficulties faced when trying to remove them all. The case showed how victims might have to file many complaints, which takes a toll. So, when dealing with non-consensual intimate images, it's crucial to think about what happens after the first upload. A good response should aim for quick removal where possible, keep records, and make sure that legitimate material isn't accidentally taken down.

3. LEGAL FRAMEWORK GOVERNING IMAGE-BASED ABUSE IN INDIA

4.1 Constitutional Protection of Privacy and Dignity under Article 21 Article 21 protects the right to life and personal liberty. In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Supreme Court said that privacy is a fundamental right. This is closely tied to dignity, autonomy, and personal liberty. The judgment provides a constitutional foundation for considering what happens when images are shared without consent, and how that affects someone's right to control their own

3 Sanna, Silvia Lucia, et al. "Pixel perfect or perfectly fake? exploring the robustness of digital forensic tools against facial deepfakes and morphed images." 2025 33rd European Signal Processing Conference (EUSIPCO). IEEE, 2025.

information and avoid uncomfortable situations. Although this case wasn't about image-based abuse, the principles from it can be applied to digital privacy issues. Article 21 doesn't always apply to everyone

involved in sharing an image. The specific law used, the facts of the case, and the remedy needed all matter. Still, the constitutional right to privacy and dignity is a strong argument for taking image-based abuse seriously.

4.2 Freedom of Speech and Expression under Article 19(1)(a) and Its Limitations4 Article 19(1)(a) gives everyone the right to freedom of speech and expression, including online. This right is vital in a democracy, supporting open debate, journalism, criticism, and information sharing. Article 19(2) allows limits on this right in certain situations, such as defamation (including online defamation) and to protect dignity, reputation, and privacy. Courts must balance the right to free speech with the right to privacy. While controversial statements shouldn't automatically be treated as criminal, freedom of speech must also be limited to prevent non-consensual sharing of explicit material. Still, these limits shouldn't be used as an excuse to broadly censor speech. The Supreme Court's decision in Shreya Singhal v. Union of India (2015) clarified this. The Court struck down section 66A of the IT Act because it was too vague and could be used to ban almost any online speech. The ruling was a warning against attempts to censor India's internet community. Even so, I think the Supreme Court could have been clearer about how to interpret these constitutional protections. While I wonder if such a law could really work, it's important to have well-defined punishments and standards—without taking away basic rights from everyone just to target a few offenders. 4.3 Information Technology Act, 2000: Sections 66E, 67 and 67A The Information Technology Act, 2000, contains several provisions that may apply to particular forms of image-based abuse. • Section 66E: Violation of privacy This section deals with situations where someone intentionally or knowingly captures, publishes, or transmits images of a person's private parts without their consent. The

4 https://blog.ipleaders.in/draw-line-respect-freedom-speech-expression/

specifics depend on how "private parts" are defined in the law and whether the necessary legal criteria are met. This section can cover certain cases of non-consensual explicit imagery. However, not every image shared without consent will automatically fall under this provision. It is important to confirm that all legal requirements are satisfied for the section to apply.5 • Section 67: Obscene material in electronic form This section concerns the publication or transmission of material that is considered obscene. Whether a particular image falls under this section depends on the nature of the published content. • Section 67A: Material containing sexually explicit acts or conduct This provision addresses the electronic publication or transmission of material showing explicit sexual acts or behaviour. The application depends on how the law is worded and the specific facts of the case. If children are depicted, Section 67B may also apply, along with the Protection of Children from Sexual Offences Act, 2012. Taken together, these sections indicate that the IT Act can provide some legal remedies to address image-based abuse online. Still, not every case of non-consensual image sharing, image manipulation, or cyberbullying will be prosecuted under the same section. 4.4 Bharatiya Nyaya Sanhita, 2023: Relevant Provisions on Voyeurism, Stalking, Criminal Intimidation and Defamation There are sections within the Bharatiya Nyaya Sanhita, 2023 which are relevant. Section 77 deals with voyeurism. Section 78 addresses stalking, including repeated unwanted behavior through electronic means or surveillance. Section 79 covers words, gestures, or acts intended to insult a woman's modesty. Section 351 relates to criminal intimidation. Section 356 covers defamation. Whether these sections apply depends on the specific facts of each case. For example, if someone threatens to release intimate images, that could be criminal intimidation if the law's conditions are met. Ongoing unwanted electronic contact could be considered stalking.

5 https://www.meity.gov.in/static/uploads/2024/03/IT-Act-Rules_2000_0.pdf

Publishing an image alongside false claims of misconduct might fall under defamation. However, not every instance of trolling or offensive language will qualify as a criminal offence. Even though reputational harm is undesirable in image-based abuse cases, it may not always meet the legal definition of defamation. The

details of the behaviour, intent, legal defenses, and available evidence all need to be evaluated. In summary, the BNS is just one part of the broader legal landscape concerning digital abuse.

4.5 Intermediary Liability under Section 79 of the IT Act Section 79 of the IT Act provides certain protections to intermediaries, as long as they meet specific legal requirements. This section is especially important because digital intermediaries—such as platforms that host, transmit, index, or recommend user-generated content—are not always liable in the same way as the person who uploaded the content. How an intermediary is treated in policy terms depends on whether they are hosting or recommending content. Their liability also hinges on their role, what they know, whether they have fulfilled their duties, and how courts interpret these factors. The Supreme Court addressed questions about intermediary liability and the meaning of "actual knowledge" in Shreya Singhal v. Union of India (2015). Section 79 does not grant absolute immunity. Platforms are not automatically liable for illegal content posted by users, but their status depends on compliance with legal conditions.

4.6 IT Intermediary Rules, 2021: Grievance Redressal and Content Removal The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, set out due diligence and complaint procedures for intermediaries. Rule 3(2)(b) specifically requires action on complaints about content that "exposes private areas of any person," is "fully or partially nude," depicts "sexual activity/act," or involves "electronic impersonation" (like morphing). This rule allows for the removal of qualifying content. It's important to check the latest official version of the rules before filing a complaint, since older academic materials may refer to outdated versions. Taking down content is important, but it does not guarantee that the material will not appear elsewhere. Content can be copied to other platforms or reposted by new users.

The rules work best when the complaint process is straightforward, compliance is enforced, evidence is preserved, and repeat uploads are addressed. Also, these rules do not create criminal offences. While they require removal of certain content, they do not automatically mean the person who posted the material has committed a crime.

4.7 Civil Remedies, Injunctions and Victim Protection If the criteria for civil remedies are met, these options are available. This could include an injunction to prevent further unlawful distribution of content. Defamation claims can also be made if the shared material is defamatory. Each kind of legal remedy serves a different purpose. Requesting removal can reduce access to the content, while criminal prosecution establishes guilt and imposes punishment. Injunctions protect complainants from further harm. Civil actions can also demonstrate that someone's reputation or other rights have been harmed in a way that the law recognizes. Gathering evidence—such as URLs, screenshots, timestamps, account information, and other relevant details—is crucial to building a strong case. Working with law enforcement should be handled carefully to protect the victim from unnecessary distress. Protecting the victim's privacy is important, but the accused's rights must also be respected. Criminal and civil remedies serve different roles; for example, fast removal of content is not a criminal sanction.

4. JUDICIAL APPROACH AND CASE LAW ANALYSIS 5.1 Right to Privacy and Dignity: K.S. Puttaswamy v. Union of India (2017) In Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, the Supreme Court recognized privacy as a fundamental right under the Constitution. The Court held that privacy includes personal autonomy, dignity, and freedom. This is especially relevant where images are shared without consent, since such actions can reveal private information. While this case does not discuss liability for image-based abuse specifically, it lays the foundation for privacy as a constitutional right. This has implications for how related laws are interpreted. The decision highlights that digital privacy is not just a matter of personal preference but can also involve fundamental rights if personal or intimate information is disclosed.6

6 Patel, Animesh. "The Right to Privacy in India: Historical Evolution and Contemporary Challenges in the Digital Age." Supremo Amicus 40 (2026): 1.

5.2 Online Speech and Intermediary Liability: Shreya Singhal v. Union of India (2015) The case of Shreya Singhal v. Union of India, (2015) 5 SCC 1, dealt with issues of cyberbullying and online abuse and held that section 66A of the IT Act was unconstitutionally vague and overbroad. The case also includes a lot of commentary on intermediary liability and the application of the 'actual knowledge' test in the context of section 79 of the IT Act. This case shows the need to balance the laws of the country in order to prevent online abuse and cyberbullying on the one hand and to allow people to use their constitutional rights of free speech on the other hand. The Shreya Singhal case does not go on to deal with the manner in which section 66A is to be applied to cases of distribution of private and intimate images without consent. Thus, the application of section 66A to cases of distribution of private and intimate images without consent would be required to be dealt with in terms of the applicable law, as interpreted in various cases. This ruling can help to ensure that online abuse is dealt with effectively whilst still ensuring that people can use their constitutional rights of free speech. Laws must be applied in order to prevent online abuse whilst still ensuring that people can use their constitutional rights of free speech. 5.3 Judicial Responses to Non-Consensual Intimate Images and Morphed Content An important case to note is Mrs. X v. Union of India (W.P. (CRL) 1505/2021) [2023] DHC 2806 decided on 26 April 2023. This was a case in which the petitioner's intimate images were being circulated on the internet without her consent. The main issue for consideration was whether there was any obligation on the part of the intermediaries to remove the images of the petitioner from the internet and what were the burdens on the petitioner in order to get the images removed from the internet. The Court looked into the non-consensual circulation of the intimate images of the petitioner and examined the various options for removing the images from the internet. The Court also looked into the harm that was being caused to the petitioner by the continued circulation of the images of the petitioner on the internet. This case also recognizes that a victim should not have to be asked to accept the situation where their intimate images are being circulated online without their consent. The law must take into account the continuing effects of the images being circulated online, and the victim may have

to take steps to remove them from the online space. It is also important to note that there is a distinction between the images being hosted/indexed and being searched for. However, it cannot be assumed that all intermediaries will be held responsible in all cases. This is because the Court in the above case has analyzed the remedies available to the petitioner in detail and the burdens that the petitioner will have to discharge in each instance of the intimate images being available on the internet.

5.4 Judicial Treatment of Online Defamation and Cyber Harassment This depends heavily on the case in question. A person can be charged with defamation if a defamatory statement is published along with an explicit image of the person. A person can be charged with stalking or any other offence as provided under the relevant statute if he/she continues to contact a person without his/her consent. A person can be charged with a criminal offence if he/she has threatened to publish intimate images of a person online. Rashmika Mandanna's deepfake video was sent out to the public in November 2023. The incident was taken up by the police. It is unclear if all those involved in the scandal would be charged with criminal offences. However, it is certain that the misuse of deepfake technology could lead to severe penalties. It is a documented example of the possible penalties involved with the misuse of deepfake technology. Overall, there needs to be an analysis of the law, the specific case, the charges brought against the defendant, the investigation that was carried out, and the ruling of the court. This will help to avoid any assumptions as to whether a person will be charged with criminal offences or not..

5.5 Critical Evaluation of Existing Judicial Remedies The cases studied in this chapter all deal with different forms of online harm. The landmark case of Puttaswamy recognizes the right of an individual to privacy and dignity in terms of Article 21 of the Constitution. Shreya Singhal restricted the scope of section

66A of the IT Act on grounds of vagueness and overbreadth. Mrs. X v. Union of India dealt with the issue of non- consensual circulation of intimate images of a person on the internet. These cases acknowledge the role of the judiciary in protecting individuals from being subjected to unreasonable

restrictions to their freedom of expression and in preventing the misuse of their personal information on the internet. However, in practice, because of the complexities of the issue, the judicial remedies may not always be effective. For example, in the case of multiple websites or anonymous forums, it may not be possible to identify the person responsible for the harm within a reasonable time. Even if an order for removal is obtained from the court, the content may still be available on other websites. Thus, while the judiciary may be one of the elements of a multi-faceted approach to dealing with the issue of online harm, it needs to be supplemented by administrative and technological solutions such as effective complaints processes and efficient evidence gathering methods.

6. CRITICAL ANALYSIS OF ALGORITHMIC ABUSE AND LEGAL CHALLENGES

6.1 From Non-Consensual Dissemination to Reputational Harm

The harm caused by the publishing of non-consensual images of individuals can extend beyond the initial breach of privacy. The re-sharing and commenting on images can lead to further issues for the victim, including being made fun of, ostracized from social groups and facing difficulties in their personal and professional lives.

Consideration must be given to the extent to which events are linked and whether all instances of trolling are likely to result in defamation. A key legal issue is to understand the role of each of the parties involved in the abuse, i.e., those who published the image in the first place, those who re-shared the image and the platforms on which the image was distributed. It would be wrong to assume that all parties are responsible for the abuse.

6.2 Difficulties in Identifying Perpetrators and Preserving Digital Evidence Anonymous accounts, pretending to be someone else, deleting accounts and using different platforms can make it difficult to identify who has carried out the image-based abuse. Evidence may be removed or not available to victims. In order to carry out a proper investigation you need to ensure that you’re legally protecting any evidence you have. This will involve working with the service and having the right processes in place to gain the correct

information. You also need to make sure you are respecting people’s privacy and ensuring you are being proportionate and have due process rights. You cannot prosecute someone purely for viewing or interacting with a post. You need to look at what actions they carried out and if there are any elements of the offence in the law.

6.3 Limitations of Content Removal and the Problem of Re-Uploads While removal is a useful remedy, it will not necessarily prevent the circulation of the content. Screenshotting, downloading, mirror sites and new accounts can all be used. As seen in the Mrs. X case, asking the victim to identify every duplicate could be an unreasonable burden. However, procedures could be put in place to make removing known duplicates and duplicates easy, there can be issues with identifying the correct image from automatic matching. It is also possible that images could appear in legitimate reporting or evidence. A correct system should be put in place to make sure there is a balance between quick action and reducing the risk of incorrect removal. However, consideration should be given that removing the content, locating the perpetrators and providing compensation to the victim may be completely separate and require different remedies.

6.4 Platform Accountability for Algorithmically Amplified Harm Platforms will have an impact on the content based on their recommendation algorithms, ranking and engagement driven distribution methods however these obligations are determined by the relevant law. We must consider the nature of the platforms, how much they know about the content, how they respond to complaints, what the relevant intermediary provisions are and that they are fulfilling their due diligence obligations. The increased transparency around reporting methods and how content is moderated could help researchers and regulators identify whether responses to the identified risks are effective. Independent research could also help understand why certain features may have played a contributory factor to the disproportionate circulation of abusive content.

However, expecting them to monitor all content would be an invasion of privacy and would cause issues for legitimate expression. Accountability should be proportionate, backed up by evidence and include processes for review.

6.5 Challenges in Applying Existing Laws to AI-Generated Images AI generated images can cause many legal issues as they involve individuals in situations that may not have happened in reality. This can result in misleading, unwanted sexualization, reputation damage, and potential for harassment. Although some laws may already exist to cover certain types of abuse, this will depend on the wording of the law. An image created using AI may not meet the criteria for some obscenity, privacy or defamation laws.7 The law needs to address the difference between generating an image and distributing it. It is important to consider the level of responsibility different individuals have. One major issue is making sure the law is technologically aware but not too open to include legitimate synthetic media, satire, etc.8

6.6 Balancing Privacy, Reputation and Freedom of Expression This is a complicated area as we have a right to our privacy and our reputation but also freedom of speech. However, not everything that causes offence or embarrassment should be illegal. Freedom of speech may be an issue when dealing with journalism, criticism, art and reporting in the public interest. However, just because we have freedom of expression doesn't mean we can circulate private images without consent or engage in other unlawful forms of harassment. Principles such as simplicity and proportionality should be applied. The remedies to this should be focused around the seriousness of the breach considering the content, invasiveness, legality and public interest.

7 He, Xiangwei, and Lijuan Fang. "Regulatory challenges in synthetic media governance: Policy frameworks for AIgenerated content across image, video, and social platforms." Journal of Robotic Process Automation, AI Integration, and Workflow Optimization 9.12 (2024): 36-54. 8 Lendvai, Gergely Ferenc, and Gergely Gosztonyi. "Algorithmic bias as a core legal dilemma in the age of artificial intelligence: Conceptual basis and the current state of regulation." Laws 14.3 (2025): 41.

We should use a human rights-based approach so that victims will have protection against legitimate breaches but also so that platforms and authorities aren't overly restricting any lawful content. We should aim to offer effective redress.

7. FINDINGS AND RECOMMENDATIONS

7.1 Key Findings of the Research Non-consensual images can cause further problems when circulated and commented on. The algorithm may cause more problems than it solves in terms of the recommendation and engagement-based distribution of images, but evidence must be provided to support such a claim. Indian law has multiple protections available including constitutional rights, criminal offences, duties owed by intermediaries and civil remedies. These will depend on the circumstances. While removal of content is a key remedy to address the harm caused by image- based abuse, enforcing such removal can be difficult, as the content can be re-uploaded, uploaded anonymously, or distributed internationally. Thus, the law must

balance the right to privacy and dignity with the right to freedom of speech, as well as ensure fair procedures and protection against the removal of lawful content.

7.2 Strengthening Legal Remedies for Image-Based Abuse 1. To improve victims' ability to access and utilize current remedies, clear directions should be provided to guide victims of image-based abuse. This will allow victims to understand how they can report the abuse, what resources are available to them and what issues they need to address. The guidelines should also clearly explain the difference between requesting content removal, prosecuting an offence and using civil law remedies. Platforms, law enforcement and relevant agencies should work more closely together to ensure that victims are not having to endure lengthy and multi-pronged processes. 2. Current laws should be carefully reviewed to ensure there are gaps in the law that need to be addressed. If any loopholes are found, the bills should be written in a way that means the specific behavior is criminalized but does not create too much overlap or unclear offences.

7.3 Improving Content Reporting and Removal Mechanisms Provide detailed description of the reporting, moderation and removal processes of the platform. Conduct independent research and audits to ensure that the recommendation system does not cause proliferation of inappropriate content. Transparency must be proportionate to the risk of such harm, i.e. it must not include commercially sensitive information or compromise legally implemented security measures. Remedies must be provided to those who report such content and incorrect information must be corrected. Liability should depend on how involved the company is in distributing illegal material and whether they have taken any steps to prevent this. There would be no liability for having an algorithm.

7.4 Enhancing Algorithmic Transparency and Platform Accountability Platforms should provide detailed descriptions on their reporting, moderation and removal processes. By conducting independent research and audits we are able to ensure the recommendation system doesn't cause proliferation of inappropriate content. Transparency should also be proportional to the risk of this happening. This should not include commercially sensitive information or compromise legally implemented security measures. The processes should also outline what remediation will be provided to those who report and how incorrect information will be corrected. Liability should depend on how involved the company is in distributing illegal material and whether they have taken any steps to prevent this. There would be no liability for having an algorithm.

7.5 Victim-Centered Remedies and Institutional Measures Victim-centered measures should be applied so that individuals are not unnecessarily exposed to sensitive content and are able to report abuse easily. Victims should also have a clear understanding of the remedies available to them, which authorities can ensure through providing clarity. Training should be provided for investigators and relevant officials to increase understanding of how to handle cases of image-based abuse sensitively and the issues faced by those dealing with synthetic media.

Digital literacy programs should be made available to increase awareness of consent, privacy, redistribution and risks involved with AI generated imagery. Educational establishments, civil society and platforms can play a part in preventing abuse. International collaboration should be put in place when dealing with abuse across different jurisdictions, ensuring legal processes are respected and individuals' rights are upheld.

8. CONCLUSION

The leaking and sharing of photos of individuals without their consent is a serious threat to their personal life, dignity and reputation. This content can be continuously shared online, causing serious online bullying, harassment and defamation. The Information technology act, 2000, Article 21, Bharatiya Nyaya Sanhita, 2023, the IT Intermediary Rules, 2021 provide some measure of justice in India. Cases such as K.S. Puttaswamy, Shreya Singhal and Mrs. X v. Union of India have provided some justice. Yet victims still struggle to identify the perpetrators and ensure they receive justice quickly. Digital abuse is continuous,

therefore more accountability must be enforced on platforms and victims must have a clear process to obtain evidence and ensure that it is kept. Indian legal system needs to be more responsive towards technology to ensure digital abuse cannot occur. This should be done without causing censorship and ensuring the fundamental rights of individuals are preserved.

REFERENCES AND BIBLIOGRAPHY

A. Books and Academic Articles

1. Fido, Dean, and Craig A. Harper. Non-consensual Image-based Sexual Offending: Bridging Legal and Psychological Perspectives. Palgrave Macmillan, 2020. Google Books. 2. McGlynn, Clare, and Erika Rackley. "Image-Based Sexual Abuse." Oxford Journal of Legal Studies, vol. 37, no. 3, 2017, pp. 534–561. https://doi.org/10.1093/ojls/gqw033. 3. Halder, Debarati, and Subhajit Basu. "Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India." Information & Communications Technology Law, vol. 34, no. 2, 2025, pp. 163–186. https://doi.org/10.1080/13600834.2024.2408914. 4. Yadav, Nidhi, and Anushka Singh. "Digital Abuse and Human Rights: Legal Protection of Women and Children in Online Spaces." Indian Journal of Integrated Research in Law, 2026. Full text. 5. Hussain, Abdullah-Al-Monzur, and Tanjuma Mohima. "Cyberbullying, Social Stigma, and the Law: A Socio-Legal Analysis of Psychological Harm in Digital Spaces." International Multidisciplinary Book Series, vol. 4, 2026, pp. 141–185. Full text. 6. Wright, Michelle F. "Cyberbullying: Bullying in the Digital Age." In Handbook of Research on Individualism and Identity in the Globalized Digital Age, IGI Global, 2017, pp. 50–70. https://doi.org/10.4018/978-1-5225-0522-8.ch003.

B. Legislation

1. Constitution of India, arts. 19(1)(a), 19(2) and 21. 2. Information Technology Act, 2000, ss. 66E, 67, 67A, 67B and 79, where applicable. 3. Bharatiya Nyaya Sanhita, 2023, ss. 77, 78, 79, 351 and 356, where applicable. 4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended. 5. Protection of Children from Sexual Offences Act, 2012, where applicable.

C. Judicial Decisions

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. 2. Shreya Singhal v. Union of India, (2015) 5 SCC 1. 3. Mrs. X v. Union of India, W.P. (CRL) 1505/2021, Delhi High Court, decided 26 April 2023, neutral citation 2023:DHC:2806.

D. Official and Research Websites

1. India Code — https://www.indiacode.nic.in/ 2. Ministry of Electronics and Information Technology — https://www.meity.gov.in/ 3. Indian Kanoon — https://indiankanoon.org/ 4. Google Scholar — https://scholar.google.com/ 5. UN Women — https://www.unwomen.org/en 6. National Cyber Crime Reporting Portal — https://www.cybercrime.gov.in/ 7. https://www.prashantmali.com/cyber-law-blog-india/cyberbullying-and-trolling-in-the- age-of-ai-legal-and-social-remedies 8. https://www.preprints.org/manuscript/202409.1882 9. https://link.springer.com/article/10.1007/s44202-026-00585-y 10. https://ijlsss.com/digital-privacy-at-risk-examining-indias-legal-response-to-the-non-consensual-sharing-of-intimate-media/ 11. https://www.thehindu.com/news/cities/Delhi/delhi-police-files-fir-in-rashmika- mandanna-deepfake-case/article67522778.ece