LEGAL LOCK JOURNAL

2583-0384

VOLUME 4 || ISSUE 5

2025

‘LINK PLEASE?’: THE NORMALIZATION OF REVENGE PORNOGRAPHY AND NON-CONSENSUAL IMAGE SHARING IN INDIA

Bishakha Biswas[1]

ABSTRACT

The proliferation of non-consensual intimate images (NCII) or revenge pornography on digital platforms and AI has increased dramatically, turning ‘deepfakes’ into reproducible information that spreads rapidly and causes gendered harm. While both the Code of Criminal Procedure, 2023 and the Information Technology Act, 2000 (Sections 66E and 67) cover various aspects of online abuse, Indian law treats these acts as obscenity, defamation or indecent exposure; it mischaracterizes the accuracy with which it describes the harm, while the legal frameworks of Australia’s state-level image-driven harassment laws and the UK’s Criminal Justice and Courts Act 2015 deal with victim-centred processes with harsh penalties for explicit content.

This paper uses an analysis to argue that the existing system does not adequately address the impacts of digital sexual abuse. According to the National Crime Records Bureau’s Crime in India 2022 report, 6,896 cases were registered on charges of broadcasting obscene or sexually explicit content, many of which involved sharing intimate images without consent. Judicial responses such as ***State v. Anand*** (Kerala High Court, 2016) highlight the challenges of enforcement and evidentiary hurdles.

This paper argues that a specific legislative amendment to the information technology framework is required for strong protections, with specific separate provisions for NCII. The proposed amendments aim to provide survivor-centric mechanisms including penalties, including access to legal aid with compensation and criminal liability for threats of dissemination, significant protections against technology-enabled sexual violence in modern India, and align cyber laws with constitutional protections of privacy and dignity.

Keywords: Amendment, Digital Sexual Violence, Non-Consensual Intimate Image Sharing, Revenge Pornography, Legal Gaps, Indian Legal Framework, Discrimination Based Violence.

[1] The author is a student of law at Dept. of Juridical Science, JIS University, Kolkata.

INTRODUCTION:

"Link?" – a short and seemingly casual phrase that often appears in the comments sections of social media platforms and online forums reveals the disturbing reality of contemporary digital life. Behind this claim is the dissemination of intimate images, often taken without consent, turning private moments of trust into public displays. And this seemingly[2] minor practice of online friction is symptomatic of[3] a more common and increasingly accepted form of digital sexual violence. In a world of rapidly growing internet access and citizen engagement in social media, digital space has become a vast space for violations against privacy, consent and bodily autonomy.

Statistical trends show that there is scope for abuse through cyber in the Indian context. According to recent crime data, the incidence of cybercrime has increased sharply, from ***27,248 cases in 2018 to over 65,893 cases in 2023*** as technological developments have increased criminal activity on the digital frontier of criminal activity. ***In 2023, 4,48,211 cases*** of crime against women were reported in India, with a ***national crime rate of 66.2 per lakh female population***, showing that efforts to tackle gender-based violence are still proving elusive in both the physical and digital spheres. In the digital sphere in particular, research indicates that nearly 60% of Indian women who use the internet have experienced some form of online harassment, and the number of cybercrimes directed at women has increased dramatically in the last ten years. Further research has shown that more than 90% of victims of non-consensual pornography in India are women, highlighting the gendered nature of image-based abuse[4].

The advancement of new technologies has exacerbated this problem. According to an AI-generated explicit content report, 93% of deepfake pornography circulating online targets women. This shows how new digital tools are rapidly being used as weapons against female identities and bodies. These statistics show that digital sexual violence is a systemic problem that is not just an isolated or rare event in the larger architecture of digital interactions and gendered power[5].

[2] National Crime Records Bureau, Crime in India 2022, statistical report
[3]Nicola Henry, Asher Flynn and Anastasia Powell- Image based sexual abuse study(Routledge 2019)
[4] Clare McGlynn and Erika Rackley, Image basedsexual abuse 2017, Oxford Journal and Legal Studies
[5] Anita Gurumurthy and Nandini Chami, Gender and digital rights and the politics of online abuse, 2019.

One of the most common forms of this technology-enabled sexual abuse is revenge pornography and non-consensual image sharing (NCIS). Image-based abuse exploits the special qualities of digital media – permanence, replicability and rapid dissemination in contrast to traditional harassment. Once private images are posted online, they can be shared on other platforms, replicated indefinitely and preserved in digital archives, making it virtually impossible to completely remove them. As a result, victims suffer long-term psychological, social and reputational harm that goes beyond the initial act of betrayal.

In the Indian socio-cultural environment, patriarchal norms that stigmatize female sexuality and limit women's bodily autonomy further exacerbate the impact of such abuse. Intimate images are often expressed as a form of social control, shame or revenge, especially when romantic relationships end. Victims often experience severe emotional distress, social exclusion and victim-blaming, all of which can impact their personal relationships, educational prospects and career prospects. There is no specific legal framework in India for revenge pornography or non-consensual image sharing, although the incidence of image-based abuse is increasing.

The Information Technology Act, 2000 and the BNS, 2023 were not designed to regulate the complexities of digital sexual violence, although some of their provisions are occasionally applied in these situations. Because of this, victims often face isolated legal remedies, lengthy legal proceedings and considerable difficulties in ensuring the speedy removal of harmful content from internet platforms. Furthermore, an inter-disciplinary analysis shows that not everyone experiences the negative effects of digital sexual violence. Both the risk of abuse and access to legal remedies are greatly influenced by factors such as gender, race, class, sexual orientation, and geographic location. When seeking justice, women from marginalized communities and LGBTQ+ people often face increased stigma and institutional barriers.

Consequently, revenge pornography should be seen as a broader socio-legal problem that represents structural injustices in both offline and digital cultures, rather than simply a violation of privacy.

In light of this, this paper analyses revenge pornography and non-consensual image sharing in India using an interrelated socio-legal framework, highlighting the legal gaps that need urgent redress in IT laws. By examining the normalization of digital sexual violence, the structural vulnerability of victims, and the shortcomings of current legal protections, the study seeks to

emphasize the urgent need for comprehensive legislation and strong institutional mechanisms to protect dignity.

WEAPONIZING INTIMACY: UNDERSTANDING NCII OR REVENGE PORNOGRAPHY

Defining Revenge Pornography

The distribution or publication of sexually explicit images or videos of an individual without their consent is termed 'Non-Consensual Intimate Imagery' (NCII) or 'Revenge Pornography.' These images are often obtained through coercion, hacking, digital manipulation, or within the context of a mutually consensual relationship. Subsequently, these images are disseminated with the intent of dehumanizing, harassing, or blackmailing the victim, or to stigmatize them within society. Since NCII utilizes digital media as a tool to inflict psychological and reputational harm, academics and legal experts are increasingly identifying it as a form of 'technology-facilitated sexual abuse.'

Due to certain inherent characteristics of digital media such as permanence, the ease of replication, and the capacity for rapid dissemination (or 'going viral') the harm inflicted by NCII is far more far-reaching than that caused by traditional sexual offenses. Once intimate images are uploaded online, countless copies can be generated and distributed across various platforms, making their complete eradication extremely difficult. Consequently, victims often suffer from prolonged psychological distress, as these images may resurface repeatedly either as a lingering aftermath or after initial attempts to have them removed have failed.

Alongside the expansion of digital communication, this negative trend has also become an increasingly common occurrence. Research on cybercrime indicates that approximately 27 percent of internet users in India, aged between 13 and 45, have at some point fallen victim to incidents involving 'revenge pornography' or the online publication of private images without consent. Furthermore, according to data from the ***National Crime Records Bureau (NCRB)***, a total of ***6,896 cases*** have been registered involving the online publication or dissemination of pornographic or sexually explicit content. It is believed that in a large proportion of these cases, the private images were distributed without the victim’s consent. The severity of the harm caused by this type of image-based harassment has been clearly demonstrated in various studies on the impact on victims. According to a study by the Cyber Civil Rights

Initiative, 93 percent of victims reported severe emotional distress after private images were leaked online; 82 percent experienced disruption in their social or professional lives, and more than 50 percent reported suicidal thoughts.

These figures demonstrate that NCII is not just a common violation of personal privacy, but a serious form of psychological and social violence. Another important aspect of NCII is its 'gendered aspect'. The vast majority of victims of this crime are women; they are often targeted by their former partners as a means of asserting power or seeking revenge. According to statistics on online reporting of harmful incidents, the sharing of private images without consent was one of the most common forms of digital abuse accounting for about 28.2 percent of all reported harmful incidents online.

Statistical and Doctrinal Analysis: Why Specific Amendments on NCII Are Needed in India

The incidence of non-consensual intimate image sharing (NCII) in India is on the rise, highlighting a serious mismatch between the current legal framework and the reality of technology. While such crimes are prosecuted under a number of general sections of cyber and criminal laws, statistical evidence and judicial experience suggest that these sections are inadequate to address the unique features of image-based sexual abuse.

Cybercrime statistics in India show a consistent and sharp rise in crimes committed with the help of technology. According to the ***National Crime Statistics***[6], the number of reported cybercrime incidents has more than tripled in just five years from ***27,248 incidents in 2018 to over 65,893 in 2023***[7]. Within this broader crime category, the crime of creating or distributing pornographic or sexually suggestive content online which is often associated with image-based abuse has also increased dramatically.

Furthermore, data shows that women are the most common victims of image-based sexual exploitation; according to various studies, nearly 90 percent of victims of non-consensual pornography are women. Moreover, cybercrime incidents related to the sharing of sexual images and online harassment are often underreported. It is believed that only a very small proportion of victims file formal legal complaints; the main reasons for this are fear of social

[6] National Crime Records Bureau, Crime in India 2021, MEA.
[7] National Crime Records Bureau, Crime in India 2022, Statistics on cyber crime.

shame or embarrassment, fear of social consequences, and lack of trust in the legal system. These statistics highlight two important facts. First, the prevalence of digital sexual violence is increasing rapidly, in line with the use of social media and the spread of the Internet. Second, the true extent of the problem is likely much greater than the official statistics indicate which only point to structural barriers to filing complaints and seeking legal redress.

In the absence of a specific law to deal with NCII or 'revenge pornography', Indian courts have relied on a combination of various sections of the 'Information Technology Act, 2000' and the Bhartiya Nyaya Sanhita, 2023. ***Sections 66E, 67 and 67A*** of the Information Technology Act, as well as ***sections 77, 78, 108 and 356*** of the Indian Penal Code, are considered relevant laws in this regard and are often cited. Although these provisions open up certain avenues for prosecution of the offence, their original purpose was to deal primarily with issues of 'vulgarity' (invasion of privacy of others by stealth), obscenity or defamation not with the specific negative effects of sharing private images without consent. As a result, courts have often had to apply a broad interpretation of these provisions to deal with conduct that was not initially envisaged at the time of enactment.

Judicial precedent:

The ***State of Kerala v. Anand*** is a notable example of these limitations[8]. The accused in this case was accused of distributing private photographs of a woman without her consent. The state relied on the basic provisions of the current Internet law on obscenity and privacy in its argument. During the trial, the court accepted that the distribution of private photographs without consent was a serious invasion of a person's privacy and dignity. However, the case also demonstrated how difficult it is to classify image-based sexual harassment under conventional legal definitions such as obscenity or 'voyeurism'. Due to the limitations of the legal framework, the state was forced to rely on provisions that did not explicitly address the harm caused by sharing private photographs without consent.

This case demonstrates how the lack of a specific definition of the crime creates conceptual and procedural limitations; This has forced courts to deal with issues such as ‘NCII’ (dissemination of non-consensual intimate images) through indirect legal mechanisms, rather than treating them as a clearly defined statutory offence.

[8] State of Kerala v. Anand, 2026 Supreme(Online) Ker 6128.

Why the current provisions are inadequate

First, a major obstacle is the lack of conceptual clarity. While the current laws deal with the issues of 'vulgarity' and obscenity, they do not specifically recognise the specific harm caused by sharing private images without consent. As a result, the focus often shifts from the core element of the offence – 'lack of consent' to the content of the images.

Second, the rapid and widespread digital dissemination of images is not adequately addressed in the current legal framework. Within minutes of sharing them online, multiple copies of intimate images can be made and re-distributed across platforms. The current legal framework does not provide a robust mechanism to ensure that objectionable content is removed quickly or that platforms are held accountable.

Third, the law's fragmented structure leads to inconsistencies in its application and judicial interpretation. Different courts may apply different laws depending on the facts and circumstances of the case, leading to inconsistent legal outcomes.

Lastly, new technology risks like deepfake pornography, picture morphing, and AI-generated explicit content which are increasingly being utilised to produce non-consensual sexual imagery without the victim's consent are not adequately addressed by the current framework. Therefore, in order to handle severe situations, certain provisions are required.

NOTABLE INCIDENTS OF IMAGE-BASED DIGITAL HARASSMENT IN INDIA

The 'Bois Locker Room' incident (2020)

It stands as one of the most well-known examples of digital misogyny among youth in India. In May 2020, screenshots from a private Instagram group named "Bois Locker Room" went viral on social media. It was alleged that this group consisted of teenage students from elite schools in Delhi; they utilized this platform[9] to exchange photographs of their female classmates, discuss their bodies using highly obscene and sexually explicit language, and share rape fantasies with one another.

Furthermore, other members of the group were accused of inciting sexually violent behavior and circulating morphed or edited images of girls. These screenshots sparked widespread

[9] State vs Bois Locker Room FIR No. 110/2020 (Delhi police).

outrage across the country and triggered discussions among teenagers regarding misogyny, 'toxic masculinity,' and internet ethics. Following this scandal, the Cyber Crime Unit of the Delhi Police initiated an investigation. Since many of those involved in the incident were minors, authorities examined whether there had been any potential violations under the 'Information Technology Act, 2000' and the 'Protection of Children from Sexual Offences Act, 2012.'

Although subsequent investigations raised questions regarding the veracity of some of the comments, the incident nonetheless drew public attention to issues such as the normalization of misogynistic language in digital spaces and the unauthorized circulation of women's images.

The 'Sulli Deals' Controversy (2021)[10]

The 'Sulli Deals' scandal was another significant incident that exposed the misuse of women's images and harassment within the digital sphere. In July 2021, an application hosted on the software platform 'GitHub' displayed images of Muslim women; these images had been harvested from their social media accounts. By presenting these women as "deals of the day," the app essentially orchestrated a mock online auction.

This symbolic act of "auctioning off" women created a deeply dehumanizing and humiliating situation for the victims even though the platform itself did not facilitate any actual financial transactions. A significant number of the targeted women were prominent figures, journalists, and social activists; their photographs were harvested without their consent from social media accounts that were publicly accessible.

In the wake of this incident, law enforcement agencies initiated investigations; the episode also sparked widespread outrage across the country. Various provisions of the Indian Penal Code and the Information Technology Act, 2000, were invoked to address the misuse of digital platforms and the targeting of women through the unauthorized dissemination of their images.

[10] Sulli deal controversy, 2021.

The 'Bulli Bai' App Controversy (2022)[11]

The 'Bulli Bai' app controversy which once again targeted Muslim women through a mock auction website marked a recurrence of a similar incident in January 2022. Much like the preceding 'Sulli Deals' episode, the 'Bulli Bai' app collected photographs of women from social media platforms and displayed them without their consent.

This incident demonstrated just how quickly such online harassment campaigns can resurface, despite prior public outcry and legal interventions. Acting on complaints filed by the victims, both the Delhi Police and the Mumbai Police launched investigations, leading to the arrest of several individuals involved in the creation and promotion of the platform.

These two incidents are particularly noteworthy as they illustrate how—through the interplay of gender, religion, and the anonymity afforded by online identities—digital harassment can give rise to novel forms of collective and image-based abuse.

The Animesh Bakshi Case:

The case of ***State of West Bengal vs. Animesh Bakshi*** stands as one of the earliest legal precedents in India wherein the phenomenon of "revenge pornography" received formal judicial recognition[12]. This case involved a young woman whose former partner, following their separation, disseminated her private photographs without her consent.

In this instance, a romantic relationship had existed between the victim and the accused, during the course of which the accused had acquired the victim's private photographs and videos. Following their separation, with the intent to humiliate and inflict mental distress upon the victim, the accused published these private images and videos on pornographic websites and social media platforms. As a consequence of this crime, the victim suffered extreme mental anguish, and her reputation was severely tarnished.

Among the statutes applied by the West Bengal judicial court in convicting the accused was ***Section 67A*** of the Information Technology Act, 2000, which governs the publication or transmission of sexually explicit or obscene material via electronic media. Additionally,

[11] Bulli Bai app controversy, 2022.
[12] State of West Bengal vs. Animesh Bakshi, C.R.M. No. 11806 of 2017.

under the Indian Penal Code, supplementary charges were brought against the accused pertaining to offenses involving the violation of a woman's modesty or dignity.

The court sentenced the offender to five years of imprisonment and imposed a monetary fine. Furthermore, the court issued a crucial directive mandating the immediate removal from the internet of all the objectionable images of the victim that had been disseminated online. This verdict has established a significant precedent—one that acknowledges.

However, because the prosecution was forced to depend on obscenity-related statutes rather than a particular charge pertaining to non-consensual intimate pictures, the case also demonstrated the shortcomings of current legislation. This illustrates the ongoing requirement for a specific legal framework that addresses sexual assault based on images.

The Deepfake Incident of Rashmika Mandana[13]

The Rashmika Mandanna 'deepfake' incident is a recent example of how the nature of digital image-based abuse is changing. In November 2023, a distorted video went viral on social media, in which Indian actress Rashmika Mandanna was falsely shown in an offensive situation. The video was created using 'deepfake' technology; this technology digitally superimposes the actress's face onto another person's body with the help of artificial intelligence (AI).Despite being completely fabricated, the video quickly went viral on various social media platforms. It illustrates how it is possible to use new technology to create highly believable yet completely false and offensive content about well-known people. The widespread dissemination of this deepfake video has raised deep concerns among the general public and has sparked a debate about the misuse of artificial intelligence for digital harassment and sexual exploitation.

In the wake of the incident, authorities are examining possible legal action under the IT Act, 2000 particularly those sections that deal with the dissemination of pornographic or sexually explicit content online. The controversy has also prompted policymakers and digital rights experts to discuss the urgent need to impose stricter controls on deepfake technology and create a more transparent legal framework to deal with AI-generated 'NCII' (non-consensual nude or indecent images/videos).

[13] Deepfake of Rashmika Mandana controversy, 2023.

Rashmika Mandanna's case is particularly significant because it embodies the next phase of image-based sexual abuse. In this new phase, attackers no longer need actual personal images of the victim. Instead, AI can create highly realistic offensive content that causes psychological and social damage without the victim's direct participation. This incident clearly highlights the necessity of updating the existing legal framework to address the emerging forms of technology-facilitated sexual abuse.

COMPARATIVE LEGAL APPROACHES TO NON-CONSENSUAL INTIMATE IMAGE SHARING: THE UNITED KINGDOM AND AUSTRALIA

Legal Framework in the United Kingdom

Recognizing the evolving nature of digital abuse, the UK has further expanded its protective measures through subsequent legislative amendments. Later statutes such as the ***'Domestic Abuse Act 2021'*** have broadened the scope of protection; under this Act, threatening to publish intimate images is deemed illegal, even if those images have not yet been shared or disseminated to anyone[14].

Furthermore, the ***'Online Safety Act 2023'*** which mandates digital platforms to remove harmful content (including intimate images published without consent) has further enhanced the UK's regulatory framework for tackling online harms. This legislation also addresses emerging risks, such as "deepfake pornography" and other forms of sexual abuse enabled by technology[15].

The ***'Criminal Justice and Courts Act 2015'*** which introduced provisions establishing the sharing of private sexual images without consent as a specific criminal offense represented a robust legal response by the UK to the issue of "revenge pornography[16]."

Key legal provision:

Under ***Section 33*** of this Act, it is strictly unlawful to publish private sexual images or videos of another person without their consent, and with the intent to cause them distress or psychological harm. This section stands as one of the earliest legislative initiatives specifically aimed at explicitly prohibiting "revenge pornography."

[14] Domestic Abuse Act, UK, 2021.
[15] Online Safety Act, UK, 2023.
[16] Criminal Justice and Courts Act, UK, 2015.

According to the Act, an individual is guilty if:

- They purposefully reveal a private sexual image or video,
- The disclosure takes place without the person portrayer's permission, and
- The disclosure is made with the goal of upsetting or degrading that individual.

According to the statute, "sexual" images are those that portray sexual actions, expose personal body parts, or depict sexual behaviour, while "private" images are photos or videos that are not typically exposed to the general public.

The legislation acknowledges image-based abuse as a violation of privacy and personal dignity rather than just a moral dilemma by emphasising consent above obscenity.

Legal Framework in Australia

With a combination of federal and state-level laws, Australia has created one of the most comprehensive legal responses against image-based abuse. A number of Australian jurisdictions have passed legislation that expressly forbids the taking and sharing of private photos without permission.

The Crimes Amendment (Intimate Images) Act 2017, which added crimes pertaining to image-based abuse to the Crimes Act, is one such example[17].

Important Crimes in Australian Law

Three main types of behaviour are made illegal by the law:

- Taking private photos without permission
- Unauthorised distribution of private photos
- Making threats to share personal photos

Photographs or videos that depict a person's genital or anal area, breasts (for women), or someone performing a private act like having sex or using the lavatory are all considered "intimate images".

[17] The Crimes Amendment Act, Intimate Image, Australia, 2017.

This expansive definition guarantees that the legislation includes more recent types of digital harassment, such as unauthorised recordings and altered photos, in addition to classic revenge pornography.

Australia has established institutional tools to support victims of image-based abuse in addition to criminal law. Under the federal ***Online Safety Act of 2021,*** the ***eSafety Commissioner*** is a crucial regulatory body in this area. In addition to offering victims an easily accessible reporting system, the eSafety Commissioner has the authority to:

- Issue removal notices mandating that non-consensual intimate photos be removed from platforms,
- Penalise businesses financially for noncompliance, and
- Help victims get dangerous content removed from websites quickly.
- The time needed to remove abusive content from the internet is greatly shortened by this regulatory mechanism.

Because it incorporates criminal sanctions, regulatory control, and victim assistance measures, Australia's legal approach is usually considered a comprehensive framework for combating image-based abuse.

ANALYSIS OF THE SOCIOCULTURAL FACTORS THAT SUSTAIN NON-CONSENSUAL INTIMATE IMAGE SHARING (NCII) IN INDIA

The Gendered Character of NCII and Patriarchal Social Structures

The gendered nature of NCII in India reflects a broader patriarchal system that disproportionately affects women. According to data collected under cybercrime statistics, the majority of victims involved in the online publication or transmission of sexually explicit content are women. Reports indicate that globally, ***85 to 90%*** of victims of non-consensual pornography are women a trend that is also evident in India.

Cybercrime data reveals a significant rise in online offenses targeting women. With increasing internet access, complaints regarding cyberstalking, online harassment, and the sharing of private images have risen dramatically. The widening gender disparity among victims suggests that perpetrators often exploit patriarchal beliefs that stigmatize women's sexuality and link it to "honour."

Social Stigma-Related Underreporting

Studies have shown that despite the increasing number of documented cybercrimes, a significant proportion of NCII (non-consensual disclosure of intimate images) remains unreported or unreported. According to various studies***, less than 30% of victims*** of digital sexual abuse file complaints with law enforcement agencies. This is mainly because victims fear societal backlash, loss of reputation, or pressure from family members.

The social stigma surrounding sexuality or sexual expression in India further discourages victims from taking legal action. According to various surveys, almost half of female victims of cyberbullying choose to remain silent or resolve the issue privately rather than filing a formal complaint, highlighting the profound influence of cultural norms on reporting.

Growth in Online Harassment and Digital Misogyny

With the increasing accessibility of the internet in India, new avenues have emerged for gender-based harassment to rear its head. Currently, India boasts over 850 million internet users, and social media platforms play a pivotal role in the realm of digital communication. While these platforms facilitate interpersonal connections and provide opportunities for self-expression, they have also evolved into spaces where abusive language and misogynistic content spread unchecked.

According to various reports on online harassment, a significant proportion of Indian women who use social media have fallen victim to some form of online harassment—ranging from threats and unsolicited obscene messages to the circulation of doctored images. Within these online spaces, there is a strong potential for normalizing the mindset that views women merely as objects of consumption, and for fostering an environment where the non-consensual publication of private images is perceived as a means of retribution or public shaming.

Absence of awareness and digital literacy

A low rate of digital literacy regarding consent and privacy constitutes another socio-economic issue that contributes to incidents of NCII (the non-consensual sharing of private images or videos). Despite the widespread surge in internet usage across India, understanding of or awareness regarding online safety remains uneven, particularly among young users.

According to various surveys concerning internet usage, a significant segment of young internet users remains unaware of the legal repercussions associated with sharing private images without consent. Furthermore, many are not fully informed about the safeguards available to protect digital privacy, nor are they aware of the channels through which victims can file complaints. It is precisely this lack of awareness that facilitates the occurrence of dangerous online behaviors and incidents of exploitation.

LGBTQ+ People's Vulnerability

LGBTQ+ individuals are often in a particularly vulnerable position regarding online sexual exploitation. In social environments where non-heteronormative identities (identities falling outside conventional heterosexual norms) are still stigmatized, perpetrators may threaten to leak an individual's private images with the specific intent of publicly exposing their gender identity or sexual orientation.

Various studies on cyber harassment among sexual minorities have revealed that LGBTQ+ individuals experience significantly higher rates of online harassment and blackmail compared to heterosexual users. In some instances, the fear of such an identity being exposed can have far-reaching and severe consequences such as social marginalization, workplace discrimination, or rejection by family members.

Social Repercussions and Psychological Effects

According to statistical studies on cyber harassment, victims of NCII (Non-Consensual Intimate Imagery) frequently suffer severe psychological consequences. Various surveys indicate that ***more than 60% of victims*** of online sexual exploitation exhibit symptoms of anxiety, depression, or psychological distress; furthermore, many report encountering a wide range of difficulties in their personal, professional, or academic lives.

These psychological impacts are further exacerbated by the rapid dissemination of digital content. Once private images are published online, they can be copied with extreme speed and circulated across various platforms; consequently, victims develop a deep-seated conviction that their privacy is being constantly violated.

PROPOSED LEGAL PROVISIONS FOR ADDRESSING NON-CONSENSUAL INTIMATE IMAGERY IN INDIA

Proposed Solution:

The following should be specifically made illegal by a new statute:

- Taking, keeping, or sharing private photos without permission
- Threatening to use private photos as a form of blackmail or coercion (sextortion)
- Using deepfake or morphing technology to create or modify pornographic photos digitally

Such acts should be punished with five to seven years in prison and hefty fines; repeat offenders should face harsher punishments.

1. **Aggravated Offence When Committed by a Public Servant**

Where the offence is committed by a **public servant or government official**, stricter punishment should apply because such individuals hold positions of trust and authority.

Proposed provision:

1. Minimum **seven to ten years of imprisonment**
2. Immediate **suspension from public office** during investigation
3. Permanent disqualification from holding public office upon conviction

Such a provision would ensure accountability in situations where abuse of authority facilitates exploitation.

2. **Stricter Penalties When the Victim Is a Minor**

The offence should be considered an aggravated offence if the victim is younger than eighteen.

Proposed Provision:

1. Ten years in prison at minimum, with the possibility of life in prison
2. Required registration in accordance with child protection laws

3. Expedited inquiry and trial

The serious psychological and social repercussions of image-based maltreatment of children are acknowledged by this clause.

3. LGBTQ+ Victim Protection and the Criminalisation of "Outing" via Image Sharing

Image-based abuse is frequently used to "out" or expose members of LGBTQ+ communities, especially in conservative social settings where such exposure may result in violence or discrimination.

A new clause ought to make it illegal to:

1. Distribution of private photos meant to expose someone's gender identity or sexual orientation without that person's agreement
2. Threats to reveal such pictures in order to harass or coerce
3. Anti-discrimination protections and harsher penalties should be applied to the offence.

4. Liability in Situations Where Abuse Based on Images Causes Suicide or Assists Suicide

There have been instances where victims of public humiliation or blackmail due to leaked private photos suffer from extreme psychological pain and may attempt or complete suicide.

When NCII leads to suicide or an attempted suicide, there should be a particular clause establishing aggravated culpability. Under such conditions:

1. In addition to the NCII offence, the offender should face charges for aiding and abetting suicide.
2. Depending on the seriousness of the offence, the penalty might be up to ten years in prison.

The severe psychological effects of digital sexual violence would be recognised by this clause.

5**. Criminalization of Threats and Sextortion**

Intimate photos are frequently used by offenders for extortion, blackmail, and ongoing exploitation in addition to retaliation.

The following should be specifically criminalised by law:

1. Threats to publish private photos in exchange for cash, sexual favours, or other advantages
2. Persistent intimidation with exposing threats
3. Even if the photos are never made public, such activities should be punished with up to seven years in prison and hefty fines.

6. **Stricter Penalties for Repeat Offenders**

Those convicted of NCII violations in the past should be subject to even harsher punishments for subsequent offences, such as:

1. Longer periods of incarceration
2. Restriction on using specific digital platforms or services
3. Recurring digital offenders would be strongly discouraged by this clause.

Technological Approaches to Stop Non-Consensual Intimate Image Sharing (NCII)

1. Hash-Matching Technology

Through hash-matching technology, an image is converted into a unique digital fingerprint, enabling platforms to identify identical images and prevent them from being re-uploaded. Initiatives such as StopNCII.org utilize databases to identify previously reported images and halt their dissemination. The intermediary liability requirements of the Information Technology Act, 2000 which mandate that platforms remove illicit content immediately upon receiving notification can coexist effectively with such systems.

2. Content Moderation Using Artificial Intelligence

Social media companies are increasingly employing artificial intelligence algorithms to automatically detect graphic or harmful images online before they are widely shared. To

identify potentially dangerous uploads, machine learning models analyze behavioral data and visual patterns. The legal framework of the Information Technology Act, 2000 along with the due diligence obligations imposed on intermediaries to monitor and eliminate illicit digital content is complemented by these detection systems.

3. Quick Disassembly and Automated Reporting Systems

Victims can immediately submit non-consensual images through automated reporting systems, thereby enabling platforms to remove them before they spread widely. Algorithms can identify duplicate copies of an image across multiple accounts and initiate the removal process as soon as a report is received. By facilitating the rapid collection of digital evidence, such mechanisms strengthen investigative procedures under the Bharatiya Nagarik Suraksha Sanhita, 2023, and aid in the implementation of privacy and digital security regulations under the Information Technology Act, 2000.

4. Technology for Deepfake Detection

Deepfake detection systems look for digital anomalies such as pixel errors, lighting patterns, and facial movements to identify images that have been created or manipulated by artificial intelligence (AI). With the rise in the popularity of deepfake pornography, these techniques could help prevent the spread of fake sexual content created using victims. The Evidence Rules of the Indian Code of Criminal Procedure, 2023, could be used to determine the criteria for admissibility and analysis of such digital forensic information.

5. Blockchain-Powered Image Verification

Blockchain technology can create a secure and traceable record of ownership and consent of an image. By attaching cryptographic certificates to digital images, platforms can verify that the image is being shared with the consent of the person depicted in it. According to the Indian Penal Code, 2023, such technological verification process can help in legal proceedings in cases of crimes such as digital exploitation and breach of privacy.

6. Tools for Digital Literacy and Online Safety

An integral part of technological empowerment is also the need for digital literacy programmes that make users aware of the legal consequences of sharing personal information

without consent, privacy and permission. Online safety initiatives and awareness tools incorporated in social media platforms can help deter harmful digital behaviour. Raising the level of awareness among users encourages responsible use of the digital space and increases compliance with cyber laws such as the Information Technology Act, 2000.

RECOMMENDATION

A. Reforms to the Law

1. Amend NCII for Specific Criminalisation:

India should enact a specific law that makes it illegal to create, possess, and distribute intimate images of a person without their consent. While the Information Technology Act, 2000, provides for prosecution for certain violations, these laws deal more with 'obscenity' than with 'lack of consent' or lack of permission. A specific crime would ensure stricter penalties, more balanced application of the law, and a clearer definition of the crime.

2. Identification of New Technological Violations

New forms of digital abuse such as 'deepfake' pornography, image distortion or 'morphing', and sexual content generated by artificial intelligence (AI)—should also be brought under this legal framework. The law should specifically identify and criminalize digitally distorted or altered sexual images, as such abuse allows perpetrators to create intimate images of the victim without the direct participation of the victim.

3. Boosting Evidence Gathering and Cyber Investigation

The implementation of advanced digital investigation techniques is essential for the successful prosecution of 'NCII' (non-consensual intimate images or videos) crimes. Law enforcement personnel should be properly trained in evidence preservation, 'metadata' analysis and 'computer forensics'. Proper management of electronic evidence under the 'Bhartiya Sakshya Adhinyam, 2023' and effective investigation procedures under the 'Bhartiya Nagrik Suraksha Sanhita, 2023' will significantly increase the conviction rates of criminals.

B. Societal Dimensions

1. Encouraging Consent Awareness and Digital Literacy

Various educational programs need to be implemented to raise awareness about the importance of consent in the digital realm, the right to privacy and the legal consequences of sharing private images without permission. By including 'digital ethics' and 'online safety' in the school and university curricula, young internet users can learn to behave responsibly in the digital world.

2. Resolving Victim Blaming and Social Stigma

Awareness campaigns should challenge societal stereotypes that often place blame on victims rather than perpetrators. The media, civil society organizations, and educational institutions should collectively reshape the discourse in a way that respects privacy and the right to one's own body or 'bodily identity'.

3. Mechanisms for Victim Support and Rehabilitation

Social isolation and extreme psychological distress are common among victims of image or video-based abuse. By establishing confidential helplines, psychological counseling services, and legal aid programs, victims can report incidents without fear of social stigma or slander, and receive the necessary psychological and legal support.

C. Technological Liability

1. AI-Powered Content Tracking and Identification

Digital platforms should use artificial intelligence (AI) technologies or tools that can identify offensive or distorted images before they are widely disseminated online. These technologies can recognize suspicious or unusual patterns hidden in images and help prevent harmful content from being uploaded in the first place.

2. Hash-Matching Techniques to Stop Re-Uploads

Digital platforms should implement a 'hash-matching' approach; this approach converts any alleged image into a unique 'digital fingerprint' or digital identification mark. These

fingerprints enable platforms to automatically identify and block attempts to repost the same image after it has been stored in a database, greatly limiting the viral spread of private content.

3. Quick Disassembly and Reporting Systems

Social media companies should put in place effective reporting mechanisms that enable victims to report non-consensual images immediately. Platforms should be legally obliged to remove such content within a specified period of time after reporting. The requirements of the Information Technology Act 2000 should be strengthened to hold technology businesses more accountable for stopping the spread of online sexual abuse.

CONCLUSION

The advent of digital technology has radically transformed patterns of social interaction and communication; yet, simultaneously, it has paved the way for new forms of technology-facilitated sexual abuse one such example being the 'Non-Consensual Sharing of Intimate Images' (NCII). Legal precedents, such as the case of 'State of West Bengal v. Animesh Boxi', clearly demonstrate how the unauthorized dissemination of private images or information can inflict severe psychological distress, reputational damage, and long-term social repercussions upon the victim. Similarly, recent incidents involving content altered or generated by Artificial Intelligence (AI) attest to how technological advancements have further expanded the scope of 'image-based abuse.' Statistical data further underscores the growing prevalence of this issue. Over the past decade, the number of cybercrime-related complaints in India has risen significantly, with a substantial portion of these complaints pertaining to online harassment, the circulation of obscene content, and violations of personal privacy. Various studies indicate that ***approximately 90% of victims*** of non-consensual pornography are women, thereby clearly highlighting the gendered nature of sexual abuse within the digital sphere. Concurrently, the prevalence of victim-blaming and the fear of social stigma result in the underreporting of many incidents suggesting that the true extent of NCII is likely far greater than what is reflected in documented records.

Various socio-economic and cultural factors including digital misogyny, patriarchal mindsets, and a lack of awareness regarding consent and online privacy are primarily responsible for the persistence of such criminal activities. Although the legal measures under the Information

Technology Act, 2000 can only provide partial redress, emerging technological safeguards such as artificial intelligence-based identification systems, hash-matching tools and rapid takedown of objectionable content can be very effective in preventing this problem. Therefore, a multi-pronged approach is needed to address the NCII issue; one that integrates enhanced legal safeguards, technological interventions and digital awareness. In this rapidly changing digital environment, real protection of personal privacy, dignity and physical liberty can only be ensured through integrated legal, technological and social initiatives.