NON-CONSENSUAL INTIMATE IMAGE ABUSE: A CRITICAL ANALYSIS OF THE INDIAN LEGAL FRAMEWORK AND JUDICIAL RESPONSE

Khushi Awana, Amity University, Noida

ABSTRACT

Non-Consensual Intimate Image Abuse (NCIIA) has become a critical digital crime, made possible due to the fast development of online spaces where content can easily be distributed. The purpose of this paper is to explore the phenomenon of NCIIA and discuss it as an intricate form of offense, covering the illegal creation, distribution, and editing of intimate imagery, involving acts like voyeurism, morphing, deepfake, and sextortion. The key element which differentiates NCIIA from other violations is the absence of any consent at any point during the image distribution process.

The research paper examines the current legal regime in India, which includes constitutional rights and provisions, penal laws provided by the Indian Penal Code, Information Technology Act of 2000, intermediary liability principles, and emerging data protection laws. Though the laws partially address the NCIIA, several gaps emerge from the discussion. The lack of a specific law to address the matter, the focus on content-based crimes instead of injury-based crimes, gender restrictions, and the difficulties in enforcement due to the international nature of the web are all major concerns. Legal precedents have greatly assisted in broadening the definition of privacy and dignity.

Moreover, it examines the effect of recently introduced policies, including standard procedures for swift content elimination, and stresses the growing importance of data protection laws in tackling the problems associated with information privacy. Thus, it is evident that an inconsistent approach to legal intervention, which is solely reactive, fails to address the intricate issues involved in NCIIA. Therefore, the research suggests adopting a more coordinated, consensual, and victim-oriented legal strategy, undergirded by appropriate legislation, institutional development, technological responsibility, and public awareness.

Keywords: Non-Consensual Intimate Image Abuse, Digital Consent; Privacy, Legal Framework

I. Introduction

The rapid development of digital technology and the widespread presence of the Internet have changed the way human beings communicate, interact, and express themselves. With the help of tools such as social media, instant messaging applications, and digital media sharing sites, it has become easier than ever to connect with others conveniently. On the other hand, however positive such developments may appear, they have created many instances where various forms of abuse and exploitation take place through the use of digital media. One such example of an emerging form of abuse and exploitation is NCIIA, or non-consensual intimate image abuse.

NCIIA refers to acts involving the production, holding, and distribution of sexually explicit imagery of individuals without their consent. It also entails the threat of releasing such pictures to control others. Unlike other breaches of privacy, NCIIA is unique in its attributes based on the internet, whereby images can easily be spread, stored, replicated, and circulated instantly and forever. Images that are out in the internet cannot be removed once they are out there, hence making it difficult for the victim to evade.

It is important to recognize that the core principle of NCIIA lies in the uniqueness of the technology that makes it possible to transmit and reproduce information within seconds. Unlike physical attacks, digital images can be shared around the globe immediately and saved permanently on the Internet, leaving no room for removing any trace of evidence.

On the contrary to sexually exploitative acts that take place traditionally, NCIIA takes place due to advanced technologies that make it possible for people to post the content on the Internet without delay. The notion of NCIIA encompasses a variety of behaviours, which makes it relevant in contrast to other concepts like "revenge pornography" that cannot be considered as adequate descriptions of the essence behind numerous cases leading to sexual abuse.

One can describe the core aspect of NCIIA in the absence of consent throughout all stages of distribution of the pictures from creation to circulation and dissemination of the pictures. Even though the individual may have offered consent for producing the pictures or distributing the picture with someone else privately, it does not offer any grounds for publicly distributing or even giving the picture to some third party.

In addition, there exist several forms of NCIIA, among the commonest being the distribution

of intimate pictures that were created by both individuals but were distributed to other people once the relationship ended. The distribution is often motivated by feelings of revenge, embarrassment, and manipulation against the other party. However, another instance of NCIIA occurs where the other individual secretly films an act of sex between the two parties.

The next dimension of NCIIA involves the use of edited or "morphed" images. Namely, the image or face of the victim gets transferred via computer editing into the content with an explicit character. Thus, such photographs can be particularly damaging since they can harm a victim's reputation even if the images do not reflect any real-life situations. Finally, another recent phenomenon related to the use of digital technologies and NCIIA is deep faking which implies the fabrication of a video that features someone performing sexual actions, albeit it is completely untrue.

Therefore, NCIIA can be characterized as multidimensional digital abuse, encompassing a wide range of actions, distinguished by non-consensual violation of the victims' personal integrity. The various examples of NCIIA presented above show not only the complexity of this phenomenon but also some of its challenges related to its prevention. It is therefore important to know what NCIIA is and different forms of NCIIA to formulate the most effective response strategy against this problem.

II. Analyzing the legal framework in India

India’s legal response to NCIIA is multi-faceted but fragmented, including provisions in the Constitution, penal laws, cyber laws, and data protection laws. There are no comprehensive laws regarding NCIIA in India; however, a blend of various legislative initiatives attempts to counter this problem. The development of digital technologies has far outpaced any legislative intervention, creating gaps and ambiguities within the legal regime. Therefore, dealing with NCIIA from a legal perspective demands an interpretive and holistic approach by incorporating different laws.

2.1 Constitutional Protections: Right to Privacy and Dignity

The Constitution of India provides a strong normative foundation for protecting individuals against NCIIA through fundamental rights, particularly the right to privacy and dignity under Article 21. Given the present-day digital age, the content generated and stored by individuals

is prone to being abused through digital technology.

The landmark judgment of *Justice K.S. Puttaswamy (Retd.) v. Union of India*[1] firmly established the right to privacy as a fundamental right under Article 21. The Supreme Court highlighted the fact that the right to privacy not only entails the right to protect one's personal information but also encompasses bodily integrity and decisional autonomy. The importance of transparency in seeking consent was also talked about. This emphasis on informed consent is crucial in ensuring that individuals are aware of and can control how their data is utilized.[2] In the context of NCIIA, this judgment is particularly significant, as it affirms that individuals have the right to control the dissemination of their personal and intimate content. Unauthorized sharing of such content directly infringes upon this right, making NCIIA not only a statutory offence but also a constitutional violation.

Another fundamental aspect of Article 21 is the right to dignity, which is closely connected to the right to privacy. Dignity means a right to life with the sense of self-respect and autonomy, without any feelings of humiliated and degraded status. NCIIA violates this aspect of a person's dignity by exposing one's life to social criticism, mockery, and stigma. The non-consensual sharing of personal photos deprives an individual of his or her dignity, turning him or her into an object of abuse. This makes constitutional dignity rights relevant here.

Article 14 of the Indian Constitution along with Article 21, which guarantees equality before law and equal protection of laws respectively, holds importance in the context of NCIIA. This means that every person is entitled to the same legal protection from the digital violation irrespective of any difference in their gender, social standing, etc. But in light of the fact that NCIIA has affected women and marginalized communities much more than any other community, the concept of substantive equality plays an important role. It suggests that certain measures should be taken by the state to counter the inequality in society.

2.2 Indian Penal Code and Relevant Offences

Another major law in India that is used to prosecute any crime related to NCIIA is the Indian

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) 10 SCC 1.
[2] Adyasha Behera & Bhanu Pratap Singh, *Safeguarding Privacy in the Digital Era: Balancing Rights, Security, and Innovation*, 5 Chanakya L. Rev. 57 (2024), https://cnlu.ac.in/wp-content/uploads/2025/05/Safeguarding-Privacy-In-The-Digital-Era-Balancing-Rights-Security-And-Innovation-by-Ms.-Adyasha-Behera-Mr.-Bhanu-Pratap-Singh.pdf (last visited Apr. 26, 2026).

Penal Code, 1860. The Indian Penal Code is one of the major statutes in the country used to prosecute crimes. Despite its wide applicability to most crimes, the Indian Penal Code, which was formulated without consideration for digital offenses, does not have any particular provision aimed at punishing any act of NCIIA. Nonetheless, different provisions of the Indian Penal Code have been relied on to prosecute offenders of NCIIA based on their nature. Most of the provisions of the Indian Penal Code relate to personal modesty, honor, and personal security.

One of the most pertinent provisions that can be cited in such a situation would be Section 354C[3] of the Indian Penal Code (IPC), which pertains to the offence of voyeurism. The provision makes it illegal for a person to capture an image or transmit it in case of any private activity being done by a woman without her consent. The provision is more relevant in instances where there is an exchange of images between people where the victims have no idea about it. However, this provision cannot be cited in the case of photoshopped or morphed pictures of the victim. Also, it is not a gender-neutral clause and cannot be used by male victims because it only applies to women who are apprehended while performing a private conduct.[4]

Similarly, Section 354D[5] deals with stalking, including cyber-stalking, wherein several attempts are made by the accused to make contact with the victim using any electronic device. This recognizes the use of technology in gender-based offenses and provides a legal remedy against certain forms of NCIIA.

Sections dealing with obscenity such as Sections 292 and 294[6] of IPC have also been used time and again in NCIIA cases since they deal with the selling, displaying, and distribution of obscene content. The term 'obscenity' can be interpreted to cover sexual images as well. Although it has been said that obscenity is not an appropriate charge in NCIIA cases because it tends to focus more on the type of content than the lack of consent, they may be a 'double-edged sword', as victims can themselves be charged with distributing/selling 'obscene' images. Despite the unlikelihood of policemen turning around and charging their victims, the fact remains that it is only the investigating officer who has the authority to book a case, and she/

[3] Indian Penal Code, 1860, § 354C (India).
[4] Raghav Mendiratta, *Non-Consensual Sharing of Intimate Images Online: Solutions in Criminal, Media & Technology Laws*, NLU Forum Blog (2019), https://forum.nls.ac.in/slr-forum-blog/non-consensual-intimate-images-online-solutions-in-criminal-media-technology-laws/ (last visited Apr. 26, 2026).
[5] Indian Penal Code, 1860, § 354D (India).
[6] Indian Penal Code, 1860, §§ 292, 294 (India).

he need not show empathy towards the victim.

In the situation when the release of the intimate image leads to defaming the victim, the provisions in the IPC for defamation under Sections 499 and 500 will be equally applicable. In such scenarios, defamation laws will offer relief to the affected individual since his or her reputation is bound to be ruined due to publication of such content. On the other hand, Section 503 IPC on criminal intimidation applies in situations where any threat exists of releasing an intimate image of the person as a measure of coercion or blackmail.

Provisions in relation to cheating, extortion, and criminal breach of trust under IPC may also apply depending on the circumstances surrounding the case. For example, section 406 of IPC regarding criminal breach of trust can be applied where there is misuse of intimate images exchanged in good faith by the receiver. Also, extortion can be charged under section 384 of IPC when a person is made to surrender any property through coercion using images. [7]

The use of different provisions in the prosecution of cases of NCIIA has been faced by numerous challenges that make them difficult to apply. Firstly, the failure to specifically recognize image-based sexual abuse means that application of various provisions can be quite inconsistent. Secondly, victims may have challenges in proving some elements of certain offenses due to the nature of evidence involved in such cases. Finally, the gendered nature of some provisions makes them less applicable to male victims.

2.3 Information Technology Act, 2000 and Intermediary Liability

The Information Technology Act, 2000 (IT Act) is the core law in India that helps in tackling issues concerning cybercrimes, including Non-Consensual Intimate Image Abuse (NCIIA). Designed to give legal effect to electronic transactions as well as curb cybercrimes, the IT Act has adapted itself to changing digital landscapes. While the IT Act does not have a definition or provision that criminalizes NCIIA as an offense, some of the provisions of the act may be used when dealing with issues associated with the unauthorized capturing, publishing, and distribution of intimate images.

Section 66E[8] of the IT Act is one of the main clauses dealing with the violation of privacy.

[7] Indian Penal Code, 1860, §§ 384, 406 (India).
[8] Information Technology Act, 2000, § 66E (India).

According to this section, the act of knowingly capturing or publishing any image of a private part of a person is considered illegal. Even though Section 66E has a gender-neutral application, and it covers some aspects related to NCII, the narrow definition of "private areas" would make it difficult to apply this law in cases when a person was taken in an intimate posture but not revealing any private parts.

The two additional clauses of the IT Act are Section 67 and 67A[9] that are concerned about the publication/transmission of sexually explicit and obscene material using computers. According to Section 67, anyone who shares an obscene information through a computer is liable to be punished for his or her actions, while Section 67A talks about transmitting or publishing material that contains sexually explicit acts. However, just like the IPC, these sections deal with the type of information being transmitted rather than the consent of the other party.

An important part of the IT Act is its provisions regarding intermediaries, who may be considered social networking websites, internet service providers, or any organization that aids in the distribution or storage of online information. Section 79[10] of the IT Act offers intermediaries limited immunity from being held liable for any third-party content posted on their platforms, as long as they show proper diligence and lack any knowledge of any illegal activity occurring within their platforms. However, once an intermediary is notified of unlawful content, it is required to act expeditiously to remove or disable access to such material. The concept of intermediary liability has been further elaborated through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[11]

The provisions lay down certain responsibilities on the part of intermediaries such as providing redressal mechanisms, provisions for synthetically generated content, appointing compliance officers, and removing any unlawful content following receipt of complaints. Rule 3 clearly stipulates that the intermediary will notify its policies and regulations relating to privacy, informing users of its policies regarding the prohibition of publishing or hosting anything that is obscene, pornographic, pedophilic, or an invasion of the privacy rights of others, including bodily privacy. It is pertinent in case of NCIIA as these provisions call for quick steps to ensure that the circulation of the harmful image is ceased immediately. The requirement of prompt

[9] Information Technology Act, 2000, §§ 67, 67A (India).
[10] Information Technology Act, 2000, § 79 (India); *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[11] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

responses is crucial for seeking redressal by the victims.

It must be mentioned that despite all these provisions, some problems do emerge regarding effective implementation of intermediary liability. For example, problems related to delay in removal of content, lack of transparency in the process of decision-making, as well as low levels of user awareness can prove problematic. Moreover, since digital platforms are global in nature, this makes matters even more complex with regard to jurisdictional issues when it comes to the hosting of content in locations outside of India.

To summarize, the Information Technology Act, 2000 and the intermediary liability regime offer a crucial yet inadequate legislative remedy for NCIIA in India. While the Act offers tools to penalize and regulate some actions, there are notable gaps that need to be addressed.

2.4 Role of Data Protection and Emerging Digital Laws

The new laws that have been developed for data protection and digital rights in India have created another dimension of regulation for the NCIIA. While other penal laws aim at punishing wrongdoings, data laws are concerned with the processing of personal data. Intimate photos fall under highly sensitive personal data that needs to be protected. The creation of such data laws acknowledges that the misuse of personal data constitutes a violation of both criminal and data privacy laws.

The passage of the Digital Personal Data Protection Act, 2023 (DPDP Act) can also be seen as another attempt in this direction. In DPDP, some of the core principles include data processing on the basis of consent, purpose limitation, and data minimization. These principles ensure protection against the abuse of personal data, and as per the provisions of the law, individuals (data principals) have the power to decide about how much and in what manner their personal data can be collected, processed, and shared. From this point of view, the non-consensual distribution of intimate images violates data protection norms because it entails the processing and sharing of data without fulfilling its intended purpose.

The importance of data protection legislation as regards the problem of NCIIA can be found in the recognition of the significance of consent, which is legally required in such a case. It should be stated that the person to whose consent the use of pictures was addressed should have given his consent freely. Furthermore, his consent should have been given informally, specifically,

and in such a way that would allow him to withdraw it at any time. It should be noted that this point corresponds to the idea of digital consent introduced above since, even if permission to use some materials is given, it does not apply to other uses of the material.

The formulation of SOP[12] by the Ministry of Electronics and Information Technology in 2025 marks a shift in paradigm in what is essentially a new frontier of NCIIA regulation in India. Whereas previous regulatory initiatives aimed at achieving this objective had taken the legislative route, which can be described as largely reactive and abstract in nature, it is evident that with the creation of a SOP, such efforts would now follow a more practical and victim-focused path for ensuring their quick deletion from the public domain.

Besides all types of NCII covered under previous laws, which included material with nudity as well as sexual intercourse, the SoP now considers both of these categories of content, as well as "artificially morphed images". It is important to note here that at present, neither the Information Technology Act, 2000 nor the Indian Penal Code, 1860 provides any remedy for artificially tampering with images. Additionally, it establishes Timelines for Action to be taken by Intermediaries:

1. Removal or disabling access to such information as soon as they receive any complaints about it - maximum period of 24 hours;

2. Preventing the reuploading of similar or the same material by using hash matching and crawlers – for SSMIs only;

3. Reporting about all actions being taken – coordination with Sahyog portal MHA - I4C (Indian Cybercrime Coordination Centre, Ministry of Home Affairs).[13]

In the first place, time-bound obligations increase the efficacy of measures for the benefit of the victims and prevent further abuse due to viral spread of the footage. Moreover, the obligation to use hashing technology to prevent re-uploading can be regarded as a move

[12] Ministry of Electronics & Information Technology, Government of India, *Standard Operating Procedure to Curtail Dissemination of Non-Consensual Intimate Imagery (NCII) Content* (2025), https://www.meity.gov.in/static/uploads/2025/11/a2c9500ef5f8b62a43bfc68747de592d.pdf (last visited Apr. 26, 2026).

[13] Press Information Bureau, Government of India, *Press Release*, Release ID: 2188886, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2188886&reg=3&lang=2 (last visited Apr. 26, 2026).

towards pro-active prevention, unlike the current reactive approach.

Nonetheless, considering the fact that the SoP is not a legislative instrument but rather a SoP, it lacks sufficient enforceability. Also, although the SoP allows quick deletion of maliciously used content, it does not address important issues like criminal responsibility, compensation, and support for victims, which do not fall under its jurisdiction. In addition, it is also worth noting some complications arising in connection with cross-jurisdictional legislation, when footage is stored on foreign servers. All in all, SoP is a promising approach in respect of implementing NCIIA legislation.

2.5 Judicial Interpretation and Landmark Cases

Judicial interpretation has been one of the key driving factors behind the evolution of law with regard to NCIIA in India. The judiciary has made use of constitution and statutes to tackle problems related to privacy and dignity. Through judicial innovation, there has been a significant increase in the ambit of fundamental rights as well as modification of laws according to the changing times. The Indian judiciary has successfully been able to realize the gravity of digital harms and provide justice to their victims through interpretations in various judgments.

One such landmark case is Justice K.S. Puttaswamy (Retd.) v. Union of India, in which the Supreme Court clearly held the right to privacy to be a fundamental right guaranteed under Article 21 of the Constitution. The Supreme Court also stated in its ruling that “the right to privacy includes the right to control personal information, which may be linked to the person’s autonomy, physical and psychological integrity, identity, and reputation.” Shreya Singhal v. Union of India was another case which focused on testing the constitutional validity of Section 66A of the Information Technology Act, 2000.

Case State of West Bengal v. Animesh Boxi[14] is one of the earlier cases in which someone has been convicted under the NCII act in India. After the end of their relationship, Animesh Boxi was found guilty for uploading intimate pictures and videos of his ex-girlfriend without her consent. The court sentenced Boxi to imprisonment while using the term "rape survivor" for the victim. This case highlighted the importance of adopting a victim-centric approach in

[14] Order dated Mar. 7, 2018, in G.R. No. 1587/17, Court of the Judicial Magistrate, First Class, Third Court, Tamluk, Purba Medinipur (India).

dealing with NCII offenses, similar to sexual assault cases. It was insufficient merely to label the plaintiff as a "rape survivor" for receiving compensation.

In Subhranshu Rout v. The State of Odisha[15], the Court denied bail to the NCII perpetrator, emphasizing that allowing such objectionable content to persist on social media without the victim's consent directly violates a woman's modesty and right to privacy. Furthermore, the Court underscored the significance of the "Right to be Forgotten" within privacy protections, highlighting that the permanent removal of images from servers is essential to safeguarding these rights.

In Mr. X vs Union of India[16], High Court comprehensively gives a definition of NCII, highlighting its impact on the victims and revenge porn being a subset of NCII.:

"13. Non-Consensual Intimate Images (NCII) refers broadly to sexual content that is distributed without the consent of those who are being depicted in the said content. This content may or may not be taken with the consent of the individual involved, however, its dissemination is largely meant to be non-consensual and comes under the larger umbrella of cyber-harassment. Such distribution, more colloquially known by the term "revenge porn", causes psychological damage to the victim and subjects them to social ostracization and humiliation that can seriously impact the mental health of the victim. This Court will, however, refrain from using the term "revenge porn" as it is merely a subset of NCII and NCII encompasses a larger number of scenarios in which such content may be distributed. The individual whose images are shared without their consent are perceived by the public to be deserving of the violation of their privacy and bodily integrity. Further, the same level of gravity that is attached to a crime like molestation/sexual harassment is not assigned to NCII abuse as the public in general finds it difficult to conceptualize its negative impact on account of the fact that the victim's physical person remains unharmed. However, what such conceptualization tends to ignore is that victims of NCII abuse face significant life disruptions, such as loss of job, being turned away by their families, etc., which in turn radically affects their mental health. In a 2013, a self-selected study conducted by the Cyber Civil Rights Initiative on Non- consensual Pornography (NCP), it was found that 93% of NCII abuse victims suffer significant social distress, 51% experience suicidal thoughts, and 82% experience social or occupational impairment."

[15]Subhranshu Rout v. The State of Odisha, 2021(I)ILR-CUT687
[16] Mr. X vs Union of India, MANU/DE/2685/2023

Further, the court emphasizes that the presence of NCII must be traced to "originators" who are responsible for uploading and publishing the content, and NCII's spread and its continued existence on the internet can be attributed to "intermediaries" that facilitate its flow and provide other users access to it. It also suggested to set up a fully-functioning helpline—with sensitized operators—should also be set up for victims to report NCII. The operators should also have a database of registered counsellors that distressed victims can reach out to.[17]

In G vs Union of India[18], wherein the petitioner aged 19 years and school going girl who she came in contact with MP who lured her into performing intimate acts over a video call which was clandestinely recorded by MP without her knowledge or consent. The video was used to blackmail the petitioner and then surfaced online on various platforms. The court analyzed the presence of a comprehensive legal framework that address NCII in our country and stated that NCII offends the rights and dignity of the petitioner. This case highlights vulnerability of young women in digitally mediated spaces and the misuse of power and trust.

In X Corp vs Union of India[19], Court while deciding a case on social media platform stated that free speech online is not absolute and must be balanced with reasonable state regulation to protect democratic discourse.:

"*The law must walk a tight rope between perils of unregulated expression and dangers of unrestrained censorship. In that delicate balance, rests the health of Constitutional democracy. The questions raised here were not merely about statutory interpretation, but about the preservation of democratic discourse in the digital public square. The Constitution does not permit unfettered public speaking, in the garb of freedom of speech and expression."* [20]

Over these years Indian Judiciary has demonstrated a shift to recognizing NCII as a distinct violation of constitutional rights, particularly privacy, dignity, and informational autonomy under Article 21. Through the incorporation of constitutional law into the virtual world and tackling issues of consent, harm, and accountability of platforms, the judiciary has created the foundations for a more complex interpretation of cyber abuse from a legal perspective.

[17] Aarushi Mahajan, *Search Engines and Non-Consensual Intimate Images: Delhi High Court's Approach*, MediaNama (May 2023), https://www.medianama.com/2023/05/223-search-engines-non-consensual-intimate-images-delhi-hc/ (last visited Apr. 26, 2026).
[18] G v. Union of India, 2024 SCC OnLine Del 7976.
[19] X Corp. v. Union of India, 2025 SCC OnLine Kar 19584
[20] Ibid 19

However, the use of judicial interpretation as the sole means of remedy is indicative of inherent flaws that further highlight the importance of a comprehensive legal structure**.**

III. Conclusion and recommendations

NCIIA is a unique and distinct set of cyber-crime. It cannot only be regarded as "revenge pornography" but also as unauthorized distribution, voyeurism, morphing, creation of deepfakes and sextortion. In each case, the crucial factor is the lack of consent, which means that NCIIA is an informational privacy violation along with an assault of personal body autonomy and dignity, in addition to reputation. Indian laws are fragmented and reactionary to NCIIA. Laws including constitutional provisions, IPC, IT Act, and data protection laws cover certain issues of NCIIA but do not offer a concerted effort to counteract the problem. The lack of a special law means that there is no consistent application of the measures put in place and the emerging dangers such as deep fakes and morphing go unaddressed. While initiatives taken by courts are well-meaning, they cannot serve as a replacement for legislation. The Indian judiciary has established that the NCIIA falls under the category of fundamental rights, particularly right to privacy, right to dignity, and right to informational self-determination. Yet the very dependence of such an effort on judicial interpretation proves the weakness of the process itself.

Taking into account the foregoing analysis, the following suggestions are hereby made for addressing the problem faced in the current legal framework:

1. Introduction of Special and Comprehensive NCIIA Act

In India, there needs to be an introduction of a dedicated statute, which should recognize non-consensual intimate image abuse (NCIIA) as a specific crime. Article 16 of the United Nations Convention against Cybercrime explicitly states that "*Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the selling, distributing, transmitting, publishing or otherwise making available of an intimate image of a person by means of an information and communications technology system, without the consent of the person depicted in the image*"[21]. Thus, A comprehensive NCIIA Act should include the

[21] United Nations Convention against Cybercrime, Dec. 2024, United Nations Office on Drugs and Crime, https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html (last visited Apr. 24,

different types of abuse like unauthorized dissemination, voyeurism, sextortion, morphing, and deepfakes and should be gender neutral with penalty gradations for each case.

2. Inclusion of a Consent-Based Legal Framework

There should be an explicit inclusion in the legal system that the non-consent will form the basis of the offense. Any creation, storage, and dissemination of intimate data without the prior consent of the subject should invite prosecution. This ensures conformity between the legal framework and constitutional rights to privacy, dignity, and bodily autonomy.

3. Capacity Building for the Law Enforcement Authorities

The law enforcement agencies must have specialized skills in digital forensics and other aspects of cybercrimes, along with skills required for handling cases involving victims in a sensitive manner.

4. Development of a Victim-Centric Support Framework

A full-fledged support structure must be set up to help victims in terms of getting free legal assistance, psychotherapy, and rehabilitation. Legal rights like confidentiality and deletion of the information posted should be provided to victims to help address their grievances in an effective manner.

5. Integration of Data Protection Principles

It is important that data protection legislation should include provisions to protect intimate digital data as high-sensitivity personal information. It is necessary to make sure that there are provisions for strong consent, which can be withdrawn and lead to erasure of data.

6. Regulatory Framework for New Digital Technologies

There should be an obligation in the law regarding the misuse of new technology in regard to artificial intelligence as well as deepfake technology. Liability should not only cover the development of such technology but should also cover its distribution. The platforms

2026).

themselves should also be held accountable for the same.

7. Encouraging Digital Literacy and Consent Education

There must be a proper strategy to educate the general public on matters concerning consent and privacy on the Internet. This will aid in developing better practices and avoiding more instances of NCIIA.

8. Enhancing Collaboration Among Multiple Stakeholders and Internationally

There must be a framework in place that brings together multiple stakeholders to tackle the issue of NCIIA. There is also need for international collaboration and coordination.

Thus, the difficulty that comes with NCIIA does not just lie in its legal complexities; rather, the problem is the fact that such a content can move much faster than regulation ever can. In order for the law to keep up with evolving technology, it must stop being reactionary and start becoming proactive and rights-based, placing consent at the heart of its operation. Ultimately, the success of legal efforts to intervene will be determined by how quickly these efforts act, how accountable parties are made in the process, and what kind of relief victims receive. Going forward, it should no longer be about controlling damage, but about putting controls into the digital environment itself.