

**POLICY ANALYSIS OF THE ONLINE PLATFORMS ABOUT MISUSE OF NON-
CONSENSUAL INTIMATE IMAGES IN CONTEXT OF WOMEN'S RIGHTS**

Adv. (Dr) Chintan T. Pathak

Ph.D. (Law), LL.M., PGDIT, PGDTM, DCL
Techlawyer, Attorney, Cyber Security & Data Protection Consultant

Adv. Dhiya K. Trivedi

MA, LL.M., MSWC, PGJMC, PGDVS
Advocate

Adv. Mansi N. Tailor

LL.M. (Cyber Law and Cyber Crime Investigation), NFSU
Practicing Advocate
V.T. Choksi Sarvajanik Law College, Surat

ABSTRACT:

India has a long-standing cultural value of honouring women as symbols of power and dignity, reflected in traditional expressions such as “Nari tu Narayani”. Despite these deep-rooted values, the reality is that crimes against women remain profoundly severe and heinous. In the early 2000s, where most of the crime against women are related to dowry deaths, domestic violence and rape. But as the time passes and use of internet among women expand 47% raise new forms of crime against women.¹ In 2022 Cybercrime against women was marked 10.29 lakh which raised 22.68 lakh in 2024.² Online Harassment, Cyberstalking, Identity theft, Doxing and Image Morphing is now new normal.

The expanding epidemic of Non-Consensual Intimate Image (NCII) Sharing, have created a new phenomenon known as “Digital Rape Culture” that predominantly impacts women and girls psychologically, socially and economically as well. Therefore, the purpose of the research is to analyse community guidelines of major online platforms and existing rules and regulation of India to address this Issue. Moreover, the study also focuses on Usage pattern of online platform and their awareness level regarding platform policies to bridge the gap and safeguard women's rights in India.

KEY WORDS: Non-consensual Intimate Image, Cyberspace, Online Platform Policies, Artificial Intelligence, Crime against Women

INTRODUCTION

In general terms, "Non-Consensual" refers to actions taken without consent, while "Intimate Imagery" encompasses photographs, videos, or other formats including digitally altered images or synthetic media that depict nudity, partial nudity, or sexually explicit acts. Such representations violate the privacy and dignity of the individual and are classified as Non-Consensual Intimate Image. Currently, there is no specific definition of NCII in Indian or International Law. However

- Sections 74, 76, 77, and 78 of the Bhartiya Nyaya Sanhita, 2023
- Sections 67, 67A, 67B, and 66E of the Information Technology Act, 2000
- Sections 3 and 4 of the Indecent Representation of Women (Prohibition) Act, 1986
- Section 13, 14 and 15 of the Protection of Children from Sexual Offences Act, 2012

Some Common Types of NCII:

Revenge Porn:

Revenge Pornography is a form of NCII where perpetrators are commonly an ex-partner of the victim who obtains video or images in the course of a prior relationship and then publicly shame and humiliate the victim as an act of retaliation following the breakup. Such images and videos may be acquired through hacking or, in some instances, with prior consent when the circumstances are mutually agreed upon.³ *Animesh Boxi vs State of West Bengal* ⁴ is Perfect example of revenge Pornography.

Sextortion:

In case of sextortion, perpetrators often lurk in chat rooms and record victims who share or live-stream sexually explicit images and videos of themselves. They can also hack electronic or communication devices using malware to gain unauthorized access. Additionally, these may threaten you to distribute the victim's private and sensitive images/videos with their friends, family, and relatives unless the victim meets their demands.⁵

Voyeurism:

Voyeurism can be defined as the act of observing or recording a woman engaging in an act that is not of a kind ordinarily done in public and where she would usually expect not to be observed by

anyone.⁶ *Manoj Dattatray Supekar v. State of Maharashtra*⁷ represent an example of Voyeurism.

AI Generated Intimate Images:

In this instance, offenders generate nude or sexual Deepfake image or videos using artificial intelligence, driven by motives such as sexual gratification, harassment, humiliation of the victim, or to exploit the content on pornographic websites.⁸ Although such images and videos are manipulated in nature still it closely resembles the victim and appear authentic at first sight.

Virtual Assault

It is kind of harassment that occurs within virtual reality environment, where a Digital avatar or computer-generated representation⁹ is being stalked, harassed or subjected sexually explicit behaviour without her consent. According to Media reports, in early January 2024, UK police registered a case investigating an alleged “Virtual Gang Rape” of teenage girl using a VR headset while logged into a metaverse platform.¹⁰

LITERATURE REVIEW

The Researcher referred the book “**Criminalizing Intimate Image Abuse: A Comparative Perspective**” written by Gian Marco Caletti and Kolis Summerer. It was published by OUP Oxford on **11th Feb 2024**. The Authors Focuses on intimate image-based abuse as a growing digital harm that traditional criminal law struggles to address. It compares how different countries criminalize this abuse and highlights the limits of criminal law and argues for broader solutions like strengthening platform responsibility to protect victims more effectively.

_____The Researcher referred the book “**Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery**” Which is part of Routledge Critical Studies in Crime, Diversity and Criminal Justice written by Nicola Henry, Clare McGlynn, Asher Flynn, Kelly Johnson, Anastasia Powell and Adrian J. Scott. It was published on **19th April 2022**. The authors argue that image-based sexual abuse represents a significant, multifaceted digital harm that extends far beyond “revenge porn.” Drawing on extensive empirical research, they emphasize its gendered patterns and conclude that effective prevention requires integrated legal, technological, and social strategies.

The Researcher Referred book “**Between Court Orders and Platform Policies: Understanding Law Enforcement and Meta Interactions in Addressing Non-Consensual Image Disclosure Abuse**” Written by Amna Batool and Kentaro Toyama published under the proceedings of the UNENIX symposium on Usable Privacy and Security 2025 held at Seattle, WA, USA on **August 11-12, 2025**. The Author shows Meta’s Selective approach in co-operation and refuses culturally-

sensitive cases that do not fit its standard definitions of explicit content even when accompanied by valid court orders. The authors thus highlight the need for context-sensitive platform policies, better cross-border cooperation, and structural accountability to address image-based abuse globally.

The Researcher referred article **“Deepfake: They put my face on a porn video”** written by Sarah McDermott and Jess Davies. It was Published in BBC News on **20 October 2022**. The article focuses on how the face of women had been digitally edited in to a porn video without her consent and spread over the internet. More than that all her person information and addresses were published below the video.

The Researcher referred resolution adopted by the General Assembly for agenda **Countering the use of information and communications technologies for criminal purposes** in United Nation Titled **“Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes”** on **24 December 2024**. The Resolution sets an international normative standard recognizing that online violence and NCII are human rights issues requiring state-level systemic responses. It Argues that collective efforts of legal system and Online platform will help to safeguard women’s right in digital space. It also recommends that advance technologies should be utilized in certain manner to protect human rights.

RESEARCH OBJECTIVE

- To examine the effectiveness of online platform’s policies in preventing misuse of Non-consensual Intimate Image.
- To examine the Usage Pattern of Online Platforms by Women.
- To assess the level of awareness about community guideline of online platforms and awareness about reporting mechanism of cybercrimes among Women.

RESEARCH METHODOLOGY

The Researcher has adopted a mixed-method approach.

In Doctrinal Research, Researcher analyze existing laws, regulations, global standards, judicial

decisions, and policy documents related to NCII. The researcher has also examined a wide range of books, academic literature, peer-reviewed research papers, magazines, and other secondary sources.

In Non-Doctrinal Research, Researcher conducted an empirical survey among different age groups of women residing in the India. The purpose of this survey was to assess their awareness, lived experiences, perceptions, and concerns related to NCII, including psychological and social consequences, barriers to reporting, and their trust in legal mechanisms.

RESEARCH PROBLEM

To identify and bridge legal and procedural gap of Online Platforms ‘Policy in context of Non-Consensual Intimate Image (NCII) under Indian Legal Framework.

POLICY ANALYSIS OF THE ONLINE PLATFORMS ABOUT NON-CONSENSUAL IMAGES

1. Metal Policy on NCII:

Meta’s “Adult Sexual Exploitation Policy”, “Bullying and Harassment Policy”, “Child Sexual Exploitation, Abuse and Nudity Policy”, “Adult Nudity and Sexual Activity Policy” and “Sexual Solicitation policy” are part of its Community Standards which are designed to prevent and remove content that involves sexual violence, exploitation, non-consensual intimate imagery or acts, Adult Nudity, Doxxing, Sex-trafficking, Revenge Porn with non-consenting adults is disallowed under this policy.¹¹

Monthly Report of Facebook in Category of “Adult Nudity and Sexual Activity” and “Report Received” in India¹²

Month 2025	Content Actioned	Report Received	
		Content Showing me in nudity/partial nudity or in a sexual act	Content I appear in that I do not want displayed
June 2025	16 Lakh	1221	Not Available
July 2025	13 Lakh	2964	Not Available
August 2025	12 Lakh	3542	Not Available
September 2025	10.6 Lakh	2873	Not Available

October 2025	9.9 Lakh	2471	Not Available
Total	61.5 Lakh	13,071	Nil

Monthly Report of Instagram in Category of “Adult Nudity and Sexual Activity” and “Report Received” India¹³

Month 2025	Content Actioned	Report Received	
		Content Showing me in nudity/partial nudity or in a sexual act	Content I appear in that I do not want displayed
June 2025	10 Lakh	880	Not Available
July 2025	8.617 Lakh	847	Not Available
August 2025	7.3 Lakh	801	Not Available
September 2025	6.6 Lakh	741	Not Available
October 2025	7.7 Lakh	422	Not Available
Total	40.217 Lakh	3691	Nil

The report shows that Meta removes a large amount of content under the category of “Adult Nudity and Sexual Activity”. However, it fails to show how many complaints received under the category of “Content showing me in nudity/partial nudity or in a sexual act”, which mainly relate to non-consensual sharing of intimate images, are being addressed. This lack of transparency makes it difficult to understand how well Meta is responding to NCII cases.

Meta employs automated artificial intelligence systems, user reports, and specialized hash-matching technology to identify inappropriate content. However, the efficacy of AI and hash-matching technologies is limited to the detection of data that is identical to databases. Consequently, content may bypass these detection methods through minor alterations. Numerous investigative reports indicate that non-consensual images, particularly concerning ordinary (non-celebrity) women, can persist online for significant durations even after having been reported.¹⁴ Moreover, there is no public report on how effectively these tools work for content in vernacular languages or from non-Western geographies.

2. Snapchat Policy on NCII:

Snapchat Prohibits sharing, distributing, or promoting pornographic or sexually explicit content related to non-consensual intimate imagery.¹⁵ However, the major drawback of this policy is that if content is not being reported by users it might remain visible. The guidelines clearly communicate what is prohibited on its platform but do not describe how it detects or review content raising concerns about transparency and consistency.

Monthly Report of Snapchat in Category of “Adult Nudity and Sexual Activity” India¹⁶

Month 2025	Content Reported & Action Taken		Proactive Detection & Action Taken
	Content Reported	Action Taken	
June 2025	74,660	17,830	18,531
July 2025	86,042	19,416	20,940
August 2025	77,297	18,209	17,563
September 2025	76,049	17,480	18,411
October 2025	71,458	15,823	21,932

The report only focuses on “Adult Nudity and Sexual Activity” related content and fails to maintain records regarding NCII.

3. X Policy on NCII:

X’s official “Adult Content” policy permits consensually produced and distributed Adult Nudity or Sexual Behavior intended for arousal or erotic expression if it properly labeled i.e. content warning. However, if such photos used as profile photo or cover images it is prohibited.¹⁷ Practically it is not possible to determine whether distributed Adult content is consensual or non-consensual. Additionally, from technological perspective as well no algorithm or moderation tool can infer consent by examining the content alone as no content carries its consent with it.

Yearly Report of X in Category of “Non-Consensual Nudity” Globally¹⁸

Month 2024	Total No. of User Report	Action	Action Taken	
			Account Suspended	Post Removal or

				Labeled
Jan to Jun	38736	Automated	520	22,653
		Human	51,573	1,33,845
Jul to Dec	76,392	Automated	0	17,450
		Human	51,449	1,26,363

4. Google Policy on NCII:

Google NCII policy strictly prohibits Non-consensual sexual content which expose private areas, Partially or fully nude content including fake nude and any sexual act or conduct. Moreover, it also prohibits creation or generation of non-consensual intimate imagery or Deepfake using Google's AI Tools.¹⁹ However, recently in Delhi high court judgement *Mrs. X. Vs. Union of India & Ors.*²⁰ Google itself accepted that though technology is evolving but Automated detection tools are not capable of differentiate consensual and non-consensual intimate image. As Consent is not visible in photos or videos, and important details are often missing from the files. Images can also be easily altered, making it difficult to detect any changes.

Half Monthly Report of 2025 of Google in Category of "Adult Nudity and Sexual Activity" Globally²¹

Category	Content Removed
Total YouTube Channel Removed by Google due to Nudity or Sexual Act	269303
Total YouTube Videos Removed by Google due to Nudity or Sexual Act	1130927
Total Number of apps removed showing Pornograph / sexualized content (2024) ²²	7651

Although it has a policy on NCII, Google's transparency report does not provide specific data regarding NCII.

LEGAL ANALYSIS OF MISUSE OF NON-CONSENSUAL INTIMATE IMAGE OF

WOMEN IN INDIA

The Indian Constitution provides several safeguards to protect the rights and safety of women in India. Article 14 guarantees equal rights to women in India. Article 15 prohibits discrimination on the grounds of sex and allows the State to make special provisions for women. Article 21 protects the right to life and personal liberty, which the Supreme Court has interpreted to include dignity, privacy, and protection from violence. This framework empowers women's safety, equality and privacy in India.

Indian regulations address Non-consensual Intimate Image and crimes associated with it under Information Technology Act, 2000, Protection of Children from sexual offences Act, 2012, Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, Indecent representation of women act, 1986, Bhartiya Nyaya Sanhita, 2023 and Digital Personal Data Protection Act, 2023.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021²³ specifically focus on the due diligence, transparency, and accountability of intermediaries, i.e., online platforms. Rule 3 of it mandates intermediaries to remove or take down content that violates rules, promotes violence and exposes Nudity or sexual acts within 24 hours or as soon as the content is detected, whichever is lesser. However, the rule does not provide a uniform system to categories data, which makes it difficult to assess the true extent of NCII-related crimes or other cybercrimes in India. Although it mandates the swift take-

down of such content, it fails to explain what should be done when such content has already been downloaded or shared by millions of users before its removal. Additionally, the framework does not address circulation on dark-web platforms or unregulated platforms.

Recently, Ministry of Electronics and Information Technology directed SOP under clause (b) of sub-rule (2) of rule 3 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021²⁴ in line with Hon'ble High Court Judicature Madras in WP 25017/2025²⁵ to "Provide a prototype as to what a victim girl must do when faced with

situations of dissemination of NCII content”. The SOP talks about the creation of the One Stop Centre or any agency for female victims to report NCII content. However, the SOP mainly focuses on reporting procedures. It does not provide guidance on how NCII content should be detected, how platforms should prevent further circulation, or how such crimes can be effectively regulated within India.

India enacted the Digital Personal Data Protection Act, 2023 (DPDP Act), marking a significant step toward strengthening data privacy and protecting personal information online. Digital Personal Data Protection Act, 2023 explicitly talks about informed consent before collecting or processing personal data of women. However, the act right now only covers intermediaries and large data handling entities, but failed to cover an individual users who may misuse, manipulate, or share another person’s data such as intimate images without explicitly informed consent.

Some Important Cases allied to Online Harassment and Abuse against Women in India:

Ritu Kohli Case:

The Ritu Kohli Case is the First Instance of Online Harassment in India, where the accused shared her images and phone number on an online platform without her consent. However, the legal system interprets it only as "Cyberstalking", but the case involved impersonation and

misuse of a woman's personal information. The case presents a clear example of what women actually experience through it and how the justice system considers it.²⁶

Rana Ayyub Case:

Rana Ayyub is a prominent Indian Investigative journalist. She became the target of a online harassment in 2018. Someone creates a fake screenshot of a tweet falsely attributed to her and circulated it. Followed the next day someone again circulated her morphed pornographic video using her identity on all the online platforms. Her personal details were also leaked and subjected to harassment, threats and abusive calls and messages.²⁷ Despite this, case was closed stating that the “culprits could not be traced”. This incident highlights significant gaps in platform detection technologies and the failure of digital systems to prevent the rapid dissemination of non-consensual manipulated content.

Sulli Deals and Bulli Bai Case:

In this instance online app named “Bulli Bai” surfaced on 1 January 2022 that displayed photographs of more than 100 Muslim women including journalists, activists, politicians, and other public figures and listed them in a mock “auction” as if they were being “sold”. The app was hosted on an open-source code-sharing platform GitHub.²⁸ Although the “auction” was fake and no real sale occurred still the use of their image without consent with the explicit intent to humiliate and objectify, constitutes a severe crime. The fact that the content was only taken down after widespread outrage. However, several arrests were made and young man was arrested as the alleged creator of the app.

Bois Locker Room:

The “Bois Locker Room” incident involved a private Instagram group chat created by teenage boys in Delhi, India. Where underage Girls images were shared in this group. The group cha

is filled with body shaming, lewd comments, sexual assault and even rape threat. When screenshot of these chat was leaked on online platform it sparks huge public outrage. The Delhi Women’s Commission (DCW) directed the police to investigate and also asked Instagram for details about the group members and the actions taken on the platform.²⁹ Herein, Instagram fails to detect abusive words/Comments and Sexual Abuse Material Shared in that group. Another drawback is the member of the group were under eighteen.

Rashmika Mandanna Case:

In this case, a Video editor from Andhra Pradesh used Artificial Intelligence to create a Deepfake video of Rashmika Mandanna, misusing her image to simulate sexual content. This was the first instance where people began discussing Deepfakes and the dangers of AI. After that, many women's celebrity faces are being used to create Deepfake videos. Even Prime Minister Modi has also become a victim of such instances.

Rajkot CCTV Footage Leak Case:

In early 2025, footage from the CCTV system of Payal Maternity Hospital in Rajkot (and from many other CCTV-installed locations across India) was hacked and the intimate medical-examination videos of women were uploaded to porn sites and sold via Telegram/online porn networks. Investigations revealed that the CCTV dashboard hacked due to weak password. Over a span of approximately nine months, hackers reportedly accessed at least 80 CCTV dashboards including hospitals, schools, offices, homes and extracted around

50,000 video clips from various institutions nationwide. The Case raised huge concern over data privacy of women.³⁰

FINDINGS

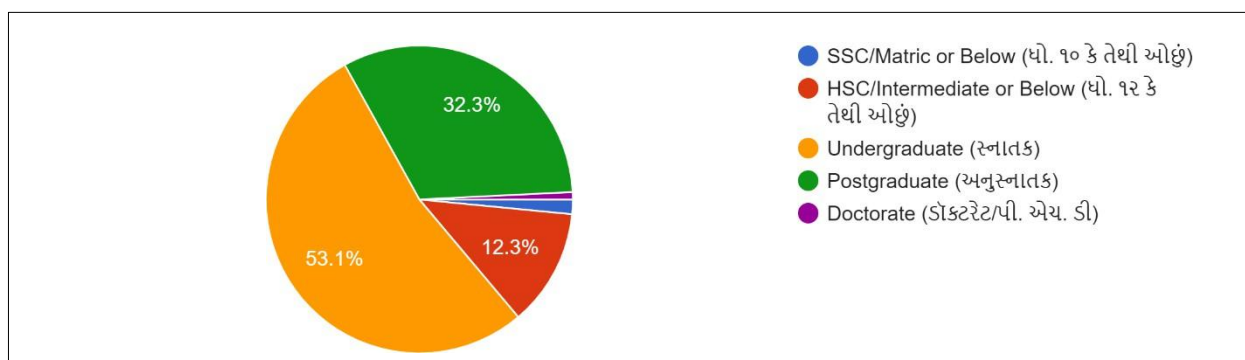
Findings from the non-doctrinal survey on “Online Platform's Policy Awareness and Rights of Women about dissemination of non-consensual Image of Women in India” conducted to know about the Usage Pattern of Online Platform, Level of Awareness and Alertness to report Cybercrime are as follows:

Sample Size:

A total of **130 Participants** responded to the Survey through Google Form.

Age Group Participated in the Survey:

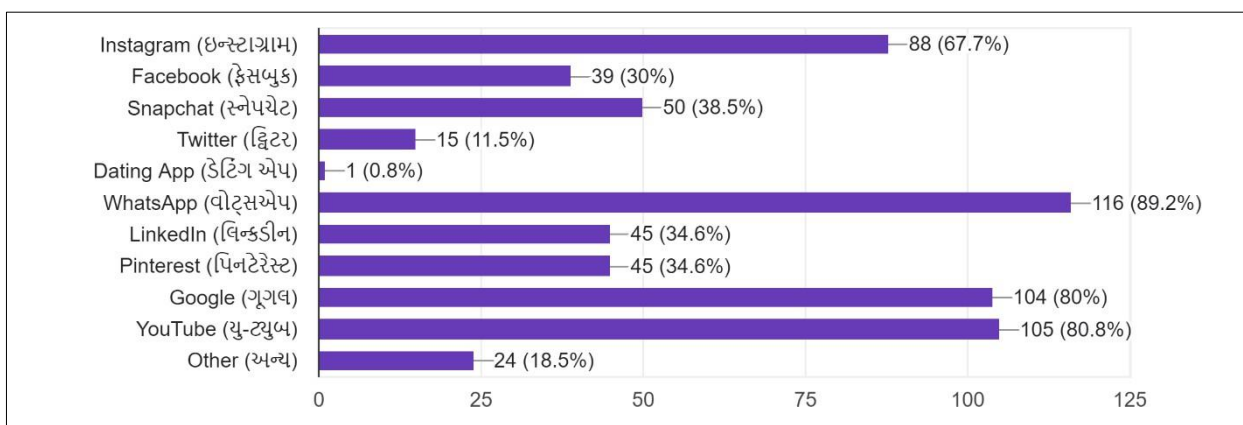
Age Group	Total No. of Women
0-18 Years	10
19-25 Years	81
26-35 Years	22
36 or More	17



Education level of Participants:

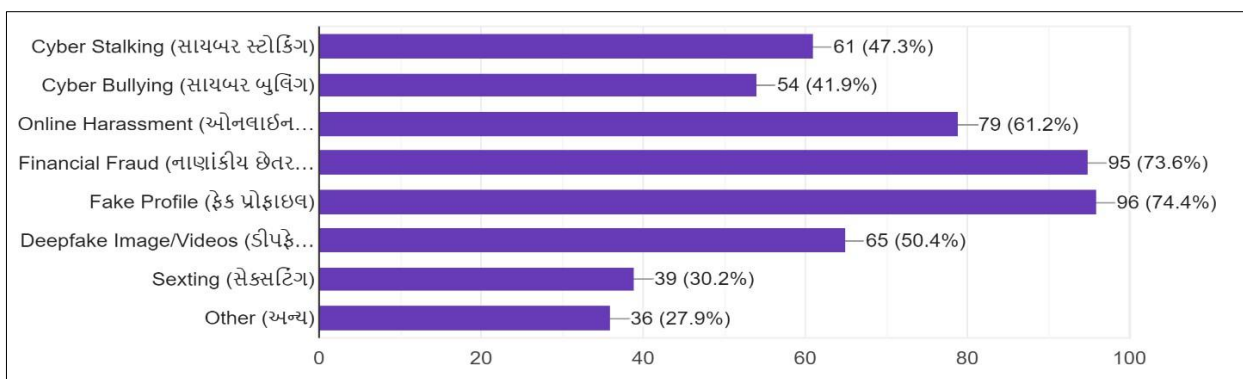
The Data Indicate that out of the total responses, 1.5% have completed SSC or below, 12.3% have completed HSC, 53.1% are undergraduates, 32.3% are Postgraduates, and 0.8% are Doctoral Holders. Overall, the sample group is predominantly composed of young and

educated women.



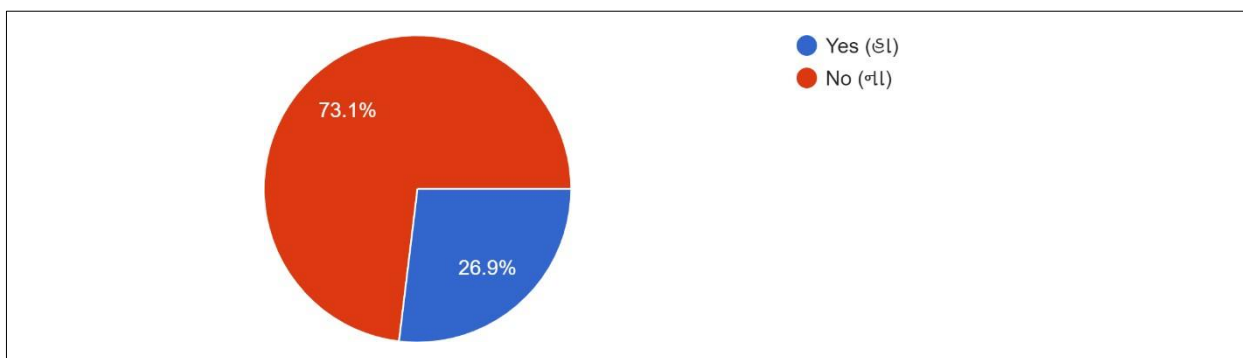
Highest Using Online Platform Among Women:

The survey indicates that Instagram, WhatsApp, Google, and YouTube are the most popular online platforms among women. This also shows that these are the platforms where women spend their time online, or those that have the most influence on them.



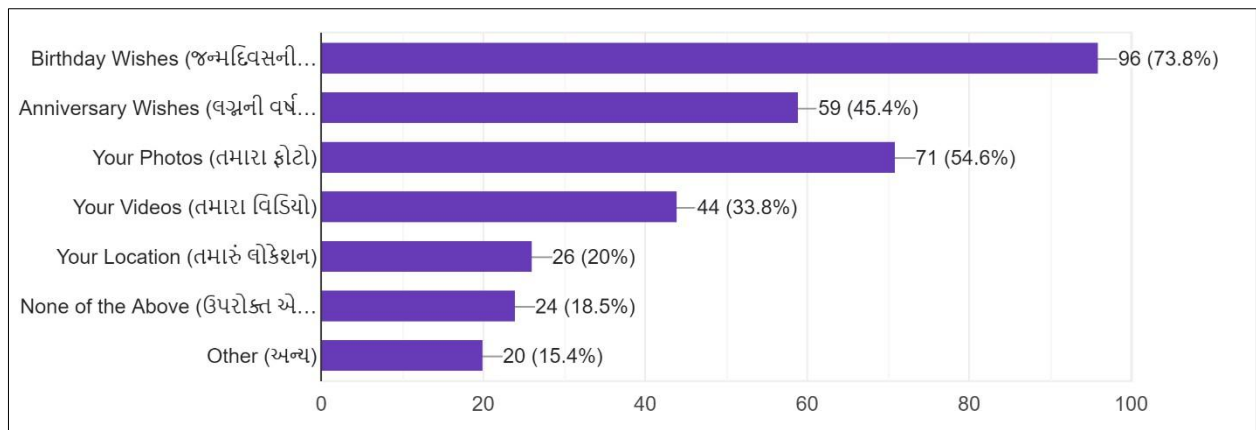
Cybercrime Awareness among Women:

The data shows that the majority of respondents know about cybercrimes such as online harassment, financial fraud, cyber stalking, fake profiling and deep-fake related crimes. On the other hand, fewer than 50% women know about sexting and cyberbullying as an offence.



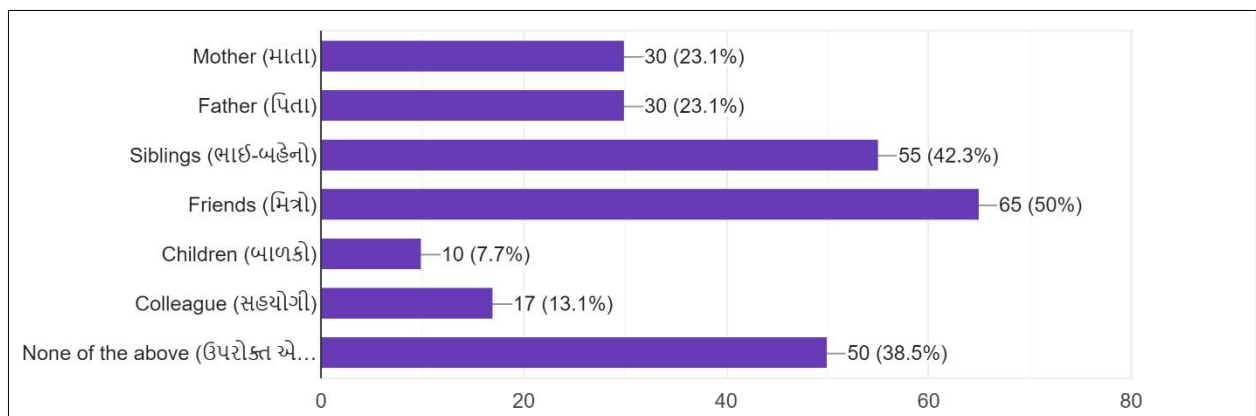
No./Percentage of Women Became Victim of Cybercrime:

The survey reveals that 26.9% of women, or women known to them, have experienced some form of cybercrime, whereas 73.1% reported no such experience. more than one-fourth of participants have directly or indirectly faced online victimization.



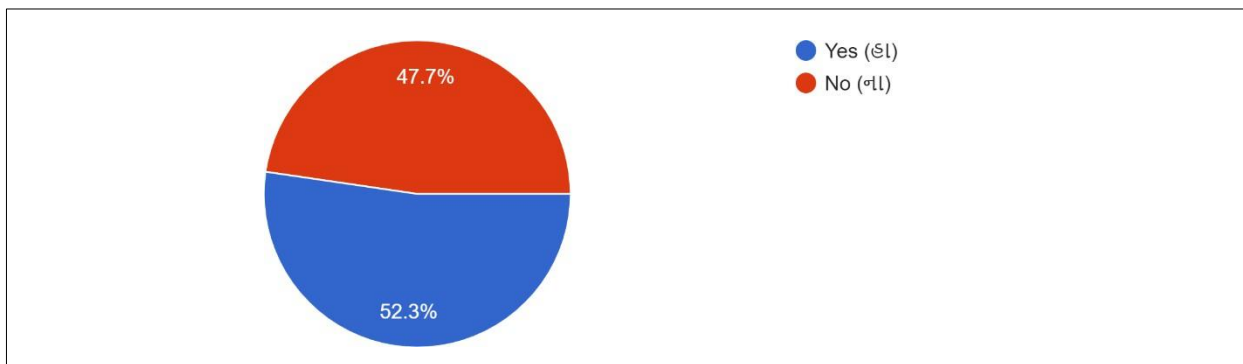
Most Shared Information on Online Platform by Women:

The Finding above indicates that most participants actively share their personal information on social media, especially birthday wishes and photographs. A few of them also share their videos, location and anniversary wishes. In contrast, only 18.5% of women reported that they do not share any personal information online. This suggests that personal information sharing remains a common practice among women.



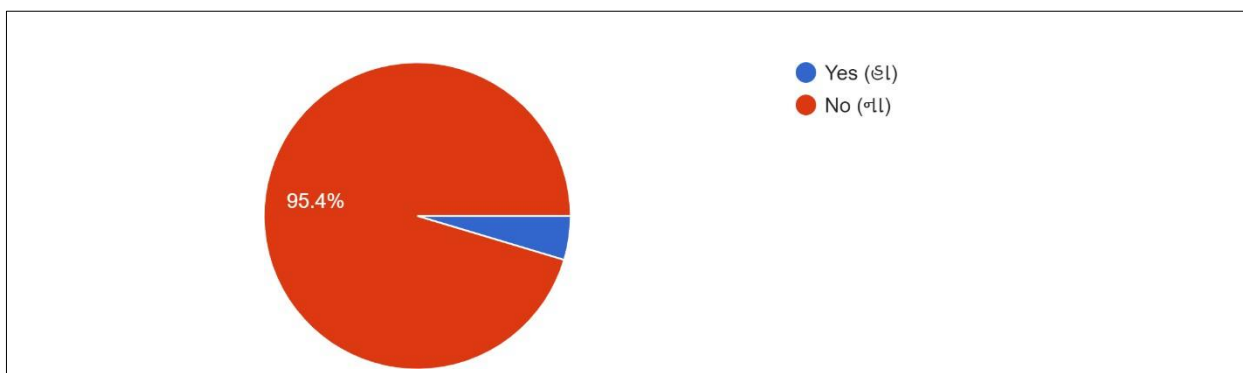
Third-Party Sharing of Personal Images/Videos of Women:

A report shockingly shows that their image/videos are shared by their friends more than their family. Specifically, 23.1% from fathers and mothers, 42.3% from siblings, 7.7% from children, and 13.1% from colleagues. Additionally, 38.5% of respondents reported that their images and videos are only shared by themselves.



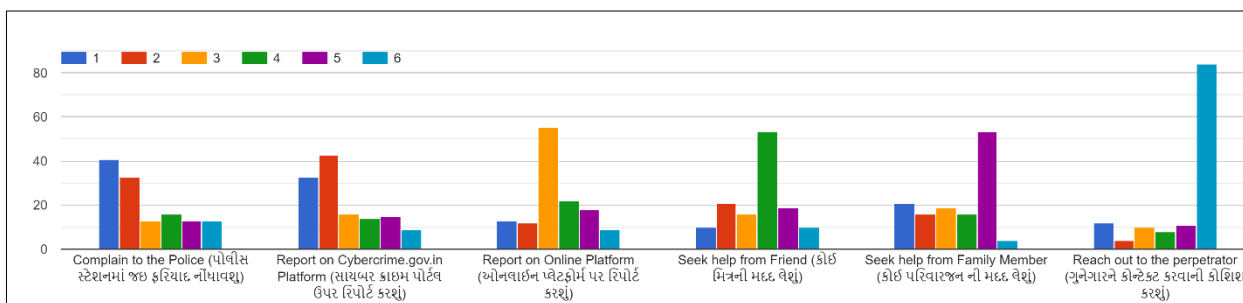
Awareness About Non-Consensual Images:

Although the respondents are active users of social media and routinely share personal information online, nearly half of them remain unaware of what NCII actually means. While 52.3% reported knowing about NCII, a significant 47.7% stated that they had no awareness of it at all.



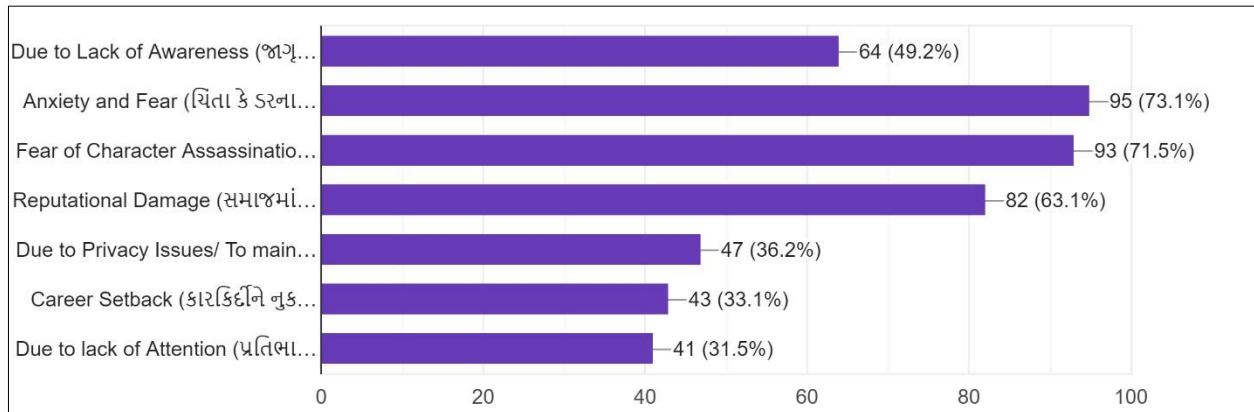
No./Percentage of Women experience Online Harassment:

The survey indicates that only 4.6% of respondents reported personally experiencing online harassment, while a significant 95.4% stated they had never encountered such incidents.



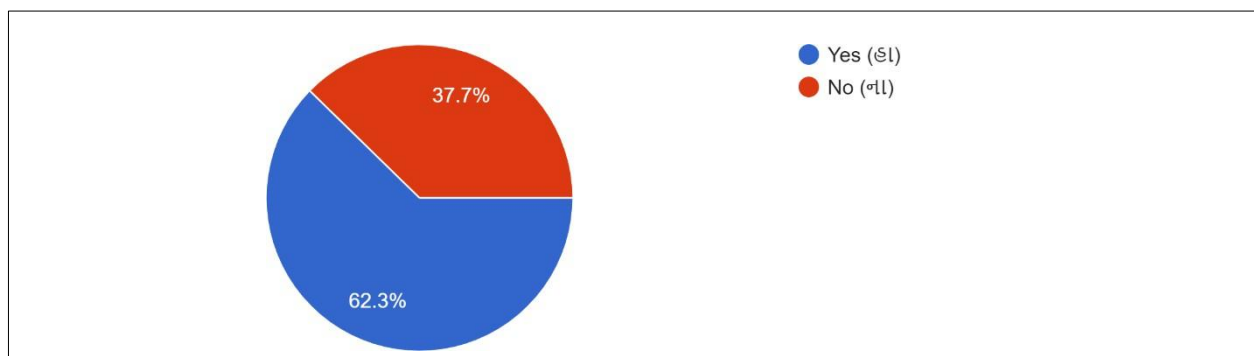
Awareness among women to report Cybercrime:

When asked about reporting behaviour in the event of NCII related crime, most of the respondent ranked their preferences in order. first, they would approach the police; second, they would report on the national portal (cybercrime.gov.in); third, they would report directly to the online platform; fourth, they would seek help from friends; fifth, they would reach out to family members; and lastly, they would consider confronting the perpetrator.



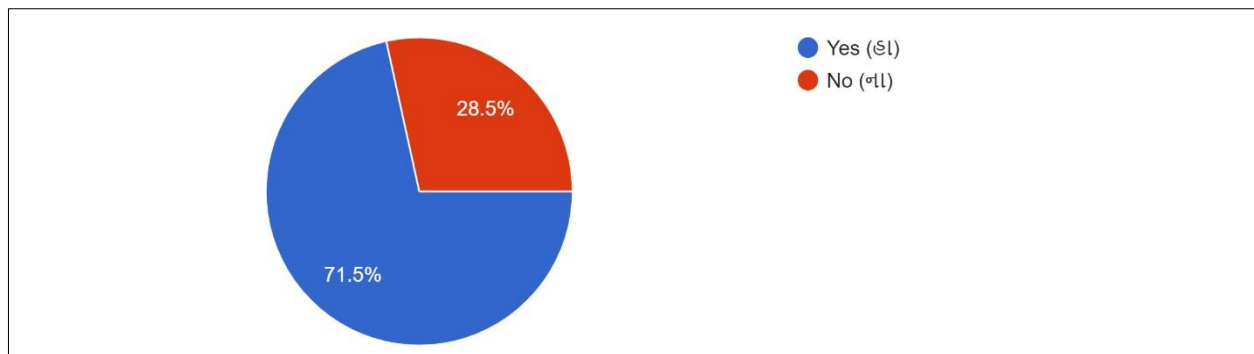
Reasons behind women afraid of reporting Cybercrime:

The survey reveals that the majority of respondents stated that they refrain from reporting incidents out of anxiety, fear of character assassination, and potential reputational harm. Additionally, 30–50% of participants indicated that other factors, such as lack of awareness of reporting procedures, privacy concerns, fear of professional consequences, and the belief that their complaints may not receive adequate attention, also discourage them from initiating a Complaint.



No./Percentage of Women feel Online Platform are unsafe for them:

A surprising finding is that even though many respondents are actively using online platforms and are aware of cybercrime risks, 62.3% still think these platforms are unsafe for women. In comparison, only 37.7% believe they are safe.



Level of Awareness on Legal Rights:

Ultimately, when it comes to legal rights, 71.5% of women are aware of them. At the same time, 28.5% are not aware of it.

CHALLENGES

- The First and Foremost challenge to address Cybercrime related to NCII in India is the lack of reporting by women. Women feel afraid to report such incidents due to social stigma, victim-blaming and fear of being humiliated in public. From the very beginning, crimes involving sexual harassment, assault and humiliation have traditionally been surrounded by shame and often expected to stay silent. However, this silence makes the perpetrator more confident to perform such an act and continue to offend.
- Many Women are unaware of how and where to report NCII-related crimes. A large number of women did not know about filing an anonymous complaint on the national cybercrime portal (Cybercrime.gov.in). They are also unfamiliar with their legal rights and the support mechanisms available to them. This challenge led to limiting the effectiveness of legal Protections.
- Rapidly evolving technologies, such as Artificial Intelligence, Deepfakes, and the Metaverse, have created new forms of NCII that are harder to detect and trace. These technologies make investigation more complex and challenging to identify the victim and the perpetrator who created it.

- The absence of a precise and comprehensive definition of Non-consensual Intimate Imagery (NCII) within the framework of Indian law presents a significant gap in the legal landscape. Existing legislation addresses certain aspects of the issue; however, it falls short in adequately addressing the complexities associated with NCII.
- Another challenge is the limitation of AI-based detection tools used by online platforms. Intermediaries heavily rely on automated systems to detect harmful content. However, AI is evolving and has not yet reached to the extent to determine whether an intimate image was shared with consent or without consent. Artificial Intelligence has its own limitations, and as a result, it sometimes fails to flag inappropriate content.
- There is a prominent rise in the number of women internet users in India. women engage more in self-expression, image and video sharing, and lifestyle comparisons online, there is a corresponding rise in the potential risks associated with the misuse of their personal information.
- Additionally, in this digital age, many individuals are forming relationships with AI chatbots and engaging in virtual reality, which presents new challenges in regulating such crimes in the Virtual World, becoming a significant challenge.
- There is uneven categorization of NCII content in platform transparency reports. Such content is often included under general categories like 'Adult Nudity and Sexual Activity' instead of being clearly identified as non-consensual intimate imagery. The reports do not provide details based on age groups, number of reports received, or actions taken, which challenges transparency and accountability on the part of the online platform.
- Online platform community guidelines are often more descriptive than applicable in practice. Sometimes content with partial nudity or that humiliates women is reported; however, the platform determine that it does not violate their community standards. Consequently, such content remains accessible online.
- Another major challenge is the viral mechanism of online platforms. Most often, images/videos fall under this category and go viral within seconds, but it takes several hours for the platform to remove them. During this time, many people download it and share it on unregulated platforms, such as the dark web or Telegram, making it extremely difficult to remove it entirely from the internet.
- Privacy vs Encryption poses another major challenge. While strong encryption is essential

to protect users' privacy and secure their personal data, it also makes it difficult for law enforcement agencies to trace and investigate cases involving NCII/CSAM. This tension between safeguarding privacy and ensuring accountability often creates gaps in timely detection, evidence collection, and prosecution.

SUGGESTION/RECOMMENDATION

- There is an urgent need to promote digital literacy among women, particularly regarding safe online behaviour, privacy settings, and the risks associated with sharing personal images or information. Many women are active on online platforms but are not fully aware of how their data can be misused, how non-consensual images can spread, or what legal rights and reporting mechanisms are available.
- Online platforms and law-enforcement agencies must simplify the reporting process so women can easily report non-consensual content without fear or confusion. Many women are unaware of the multiple channels available for help, such as platform reporting tools, the Cybercrime Reporting Portal, the Cybercrime helpline, Cyber-cells, and legal remedies. The Portal must provide user-friendly instructions and multilingual support in clear language. Awareness campaigns should focus on step-by-step reporting instructions, what happens after a complaint is filed, and how women can track the status of their case. This will increase trust and encourage more women to come forward.
- Transparency reports of online platforms currently cover NCII-related crimes under the broader Category, i.e. Adult Nudity and Sexual Activity. As per the UN Standard, it must be provided under a different Category. The Category can be improved as follows:
 - i. Age Group
 - ii. Region/Country
 - iii. Type of Content (Whether AI Generated)
 - iv. Detection Technique (AI or Human)
 - v. No. of report Received
 - vi. Action Taken

vii. Time taken for removal

- India currently lacks a clear or comprehensive definition of Non-Consensual Intimate Images. It is recommended that Indian Law should clearly define what counts as an NCII. This definition should include situations like Grooming, Deepfakes, Morphing, AI-generated Sexual Content, and even Threats to share such material. It should also cover all forms of sharing, forwarding, storing, and creating such images or videos.
- Many NCII cases involve content hosted on an unregulated platform where direct takedown is impossible. In such situations, the most effective solution is to block access from India. The law should allow authorities to immediately direct Indian Internet Service Providers (such as Jio and Airtel) to block specific URLs or IP addresses so users in India cannot view the content. Cutting access is often the only practical way to protect the victim and prevent further harm.
- On Social Media, such videos go viral very quickly, and users often download them before platforms can remove them. Intermediaries should maintain secure logs of users who download or share specific harmful URLs. This data should be provided to law enforcement agencies when required for investigation. Maintaining such records will help identify offenders and prevent further circulation on dark web, Telegram, or other unregulated platforms.

CONCLUSION

The researcher conducted this study to explore the effectiveness of online platform policies in preventing the misuse of Non-Consensual Intimate Images (NCII). Through doctrinal research, it was identified that India lacks a clear legal definition of NCII and associated crimes. The study found that online platform policies are often inadequate and complex, relying heavily on AI detection methods and showing inconsistency in transparency. While on the Non-doctrinal part, it was found that women actively use social media and share their personal information, even knowing about potential risks. Alarming, data also reveals that, their photos/videos are share mostly by their friends which increasing the risk of becoming victims of NCII-related crimes. The study also highlighted that the hesitation for non-reporting cybercrimes due to anxiety and fear of character assassination. This research offers practical recommendations, such as establishing a

clear legal definition of NCII, improving detection practices with latest tools and human interaction, enhancing reporting mechanisms, and balancing privacy concerns with encryption needs. These recommendations aim to empower all stake holders to identify and handle NCII related cases. However, the study faces limitations due to the inability to trace NCII distribution on dark-web and unregulated platforms. Future research may explore how emerging technologies create new NCII threats and whether contemporary legal framework of India address those issues. The study aims to address the legal lacuna, establish safer online platform policies, and promote awareness among users about their rights and responsibilities.

BIBLIOGRAPHY

Alice Carnevali. (2025, September 1). *Is Meta failing to protect users from the distribution of non-consensual images?* Euronews Next.

BBC News. (2020, May 4). *Bois Locker Room: Indian teens' lewd Instagram group causes outrage.* <https://www.bbc.com/news/world-asia-india-52580152>

Bhartiya Nyaya Sanhita, 2023, § 77.

Chudasama, K. (2025, December 2). *19 Minute Viral Video: સોશિયલ મીડિયાની હયમયાવી દેનારુ સત્ય આવયું સામે, અસશલ્યત તેનાથી પણ વધુ ખતરનાક.* Zee News Gujarati.
<https://zeenews.india.com/gujarati/india/19-minute-viral-video-shocking-truth-of-social-media-has-come-to-light-the-reality-is-even-more-dangerous-456020>

Debarati Halder & Basu, S. (2024). Digital dichotomies: Navigating non-consensual image-based harassment and legal challenges in India. *Information & Communications Technology Law*, 33(3), 163–186. <https://doi.org/10.1080/13600834.2024.2408914>

eSafety Commissioner. (2025). *Guide to responding to image-based abuse involving AI deepfakes (Respond 3A).*

European Institute for Gender Equality. (2017). *Cyber violence against women and girls.*

Federal Bureau of Investigation. (2025). *What is sextortion?* <https://www.fbi.gov/video-repository/what-is-sextortion/view>

Google. (2024). *Generative AI Prohibited Use Policy*.

Google. (2024). *2024 Google Play Annual Transparency Report*.

Google. (2025). *YouTube Community Guideline Transparency Report*.

Government of India. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Ministry of Electronics and Information Technology.
<https://www.meity.gov.in>

Hindu Bureau. (2024, January 4). *Virtual gang rape reported in the Metaverse; probe underway. The Hindu*.

HuffPost. (n.d.). *Deepfake porn in India: The hidden epidemic*.
https://www.huffpost.com/archive/in/entry/deepfake-porn_in_5c1201cfe4b0508b213746bd

Jaswal, S. (2022, January 2). *Bulli Bai: India's Muslim women again listed on app for 'auction'*. *Al Jazeera*. <https://www.aljazeera.com/news/2022/1/2/bulli-bai-indias-muslim-women-listed-on-app-for-auction>

Kantar & Internet and Mobile Association of India. (2024). *Internet in India 2024*.

Madras High Court. (2025, July 15). *X v. Union of India*, W.P. (Civil) No. 25017/2025.

Meta. (n.d.). *Community Standards*.

Meta Facebook. (2025). *India Monthly Report under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*.

Meta Instagram. (2025). *India Monthly Report under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*.

Ministry of Electronics and Information Technology. (2025). *SOP NCII vers.1: Standard Operating Procedure to curtail dissemination of Non-Consensual Intimate Imagery (NCII) content*. Government of India.

Mrs. X v. Union of India & Ors., 2023:DHC:2806 (Delhi High Court, April 26, 2023).

Oxford Journal of Legal Studies. (2025). From virtual rape to meta-rape: Sexual violence, criminal law and the metaverse, 45(3), 554–582. <https://doi.org/10.1093/ojls/gqaf009>

Singh, S. P. (2025, November 4). *How Rajkot hospital CCTV footage ended up on porn sites due to weak password*. Hindustan Times.

Snap Inc. (n.d.). *Community Guidelines: Sexual Content*.

Snap Inc. (2025). *India Monthly Transparency Report*.

State of West Bengal v. Animesh Boxi @ Ani Boxi @ Ani Bokshi, GR No. 1587/17 (Judicial Magistrate, 1st Class, Tamluk, Mar. 7, 2018).

Supekar, M. D. v. State of Maharashtra, Crl. B.A. No. 2131/2016 (Bombay High Court, November 23, 2016).

The Hindu Bureau. (2024, January 4). *Virtual gang rape reported in the Metaverse; probe underway*. The Hindu.

X Corp. (2024). *Adult Content Policy*.

X Corp. (2025). *Global Transparency Report*.

Kantar & Internet and Mobile Association of India. (2024). *Internet in India 2024*.

National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India Certain

crimes related to NCII are addressed through Various Provisions under Indian legal framework as below:

³ European Institute for Gender Equality. *Cyber violence against women and girls* (European Union, 2017)

⁴ *State of West Bengal vs. Animesh Boxi @ Ani Boxi @ Ani Bokshi*, GR Case No. 1587/17 (Judicial Magistrate, 1st Class, 3rd Court, Tamluk, Purba Medinipur, Mar. 7, 2018).

⁵ Federal Bureau of Investigation, *What is Sextortion?* (Video), accessed December 2, 2025, <https://www.fbi.gov/video-repository/what-is-sexortion/view>

⁶ Bhartiya Nyaya Sanhita, 2023, § 77

⁷ *Manoj Dattatray Supekar v. State of Maharashtra*, CrI. B.A. No. 2131/2016 (Bombay High Court, Nov. 23, 2016) (Jadhav, J.).

⁸ eSafety, *Guide to responding to image-based abuse involving AI deepfakes* (Respond 3A) 2025, p. 4.

⁹ From Virtual Rape to Meta-rape: Sexual Violence, Criminal Law and the Metaverse,” *Oxford Journal of Legal Studies* 45, no. 3 (2025): 554–582, <https://doi.org/10.1093/ojls/gqaf009>.

¹⁰ The Hindu Bureau, “Virtual gang rape reported in the Metaverse; probe underway,” *The Hindu*, January 4, 2024.

¹¹ Meta, *Community Standards* (n.d.)

¹² Meta Facebook. *India Monthly Report under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (2025)

¹³ Meta Instagram. *India Monthly Report under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (2025)

¹⁴ Alice Carnevali, “Is Meta failing to protect users from the distribution of non-consensual images?” *Euronews Next*, September 1, 2025

¹⁵ Snap Inc., *Community Guidelines — Sexual Content* (n.d.)

¹⁶ Snap Inc., *India Monthly Transparency Report* (2025)

¹⁷ X, *Adult Content policy* (May 2024)

¹⁸ X, *Global Transparency Report* (2025)

¹⁹ Google. (2024, December 17). *Generative AI Prohibited Use Policy*.

²⁰ *Mrs. X v. Union of India & Ors.*, 2023: DHC:2806 (Del. HC, Apr. 26, 2023)

²¹ Google, *YouTube Community Guideline Transparency Report* (2025)

²⁴ Ministry of Electronics and Information Technology. (2025). *SOP NCII vers.1: Standard Operating Procedure to curtail dissemination of Non-Consensual Intimate Imagery (NCII) content under clause (b) of sub-rule (2) of rule 3 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Government of India.

²⁵ Madras High Court. (2025, July 15). *X vs. Union of India*, Writ Petition (Civil) No. 25017/2025.

²² Google, 2024 Google Play Annual Transparency Report (2024)

²³ Government of India. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. Ministry of Electronics and Information Technology.

<https://www.meity.gov.in>

²⁶ Debarati Halder & Subhajit Basu, “Digital Dichotomies: Navigating Non-Consensual Image-Based Harassment and Legal Challenges in India,” *Information & Communications Technology Law* 33(3) (2024): 163–186, <https://doi.org/10.1080/13600834.2024.2408914>.

²⁷ HuffPost. (n.d.). *Deepfake porn in India: the hidden epidemic*.

https://www.huffpost.com/archive/in/entry/deepfake-porn_in_5c1201cfe4b0508b213746bd

²⁸ Srishti Jaswal, “Bulli Bai: India’s Muslim women again listed on app for ‘auction’,” *Al Jazeera*, January 2, 2022. <https://www.aljazeera.com/news/2022/1/2/bulli-bai-indias-muslim-women-listed-on-app-for-auction>

²⁹ BBC News, “Bois Locker Room: Indian teens' lewd Instagram group causes outrage,” May 4, 2020. <https://www.bbc.com/news/world-asia-india-52580152>

³⁰ Krushnapalsinh Chudasama, “19 Minute Viral Video: સોશિયલ મીડિયાની હયમયાવી દેનારુ સત્ય આવચયું સામે, અસશલ્યત તેનાથી પણ વધુ ખતરનાક,” *Zee News Gujarati*, December 2, 2025. <https://zeenews.india.com/gujarati/india/19-minute-viral-video-shocking-truth-of-social-media-has-come-to-light-the-reality-is-even-more-dangerous-456020>

19 Minutes Viral Video Case:

A video clip, referred to as the "19-Minute Video", began circulating widely on social media in late November 2025. The clip is said to show a couple in a private, intimate or sexual context. The video is shared, forwarded and discussed on all online platforms thousands of

times. Many girls are also being harassed, as the girl in the video resembles her. Meanwhile, cyber-experts discovered that the Video was AI-generated and created by the victim's ex-lover, who intended to take revenge.³¹

³¹ Shivam Pratap Singh, "How Rajkot hospital CCTV footage ended up on porn sites due to weak password," *Hindustan Times*, November 4, 2025. <https://www.hindustantimes.com/india-news/how-rajkot-hospital-cctv-footage-ended-up-on-porn-sites-due-to-weak-password-101762267>