Online Gender Harassment: Legal framework analysis on Revenge Porn and Sextortion

---

Table Of Contents

Abstract	1
Introduction to online gender harassment	1
Online gender harassment	1
Revenge Porn	2
Sextortion	3
Other online harassment	4
Artificial Intelligence (AI) Powered Cyber Threats	5
Impacts on victims and society	6
Analyzing the existing Indian legal framework that deals with online gender harassment	7
Information Technology (Amendment) Act 2008	13
POCSO (Protection OF Children From Sexual Offenses) Act, 2012	15
Indecent Representation of Women (Prohibition) Act, 2012	16
The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013	16
Notable Case Studies of Revenge Porn and Sextortion in India	17
Legislation From Across The Globe	18
Challenges in the legal framework	20
Policy Recommendations	20

Abstract

As internet users and influencers are growing day by day, the concern about online harassment is also increasing. Posting an opinion or expressing views regarding a specific topic has become a norm now. But in this digital realm, what comes as a reply is not limited to criticisms but threats, abusive words, and hate speech. According to recent data published by the *National Crime Records Bureau* (NCRB), India experiences more than ***500*** cases of sextortion daily. Between 2012 and 2014, there was a staggering ***104%*** surge in the sharing of revenge porn videos electronically in India. The data underscores the urgency of strengthening cybersecurity measures, enhancing law enforcement efforts, and raising public awareness to effectively combat these cybercrimes.

This research paper analyzes the Indian legal framework surrounding revenge porn and sextortion, and other online forms of gender harassment. It examines the effectiveness of existing laws, explores challenges faced by victims, learnings from legal systems across the globe, and proposes legal reforms for enhanced protection.

Introduction to online gender harassment

In India, the term "gender harassment" is not specifically defined in a separate law. Instead, the concept of gender harassment is often encompassed within the broader framework of "sexual harassment," which is addressed under the Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013. It includes any unwelcome conduct or behavior of a sexual nature by a man such as physical contact and advances, a demand or request for sexual favors, making sexually colored remarks, showing pornography, and any other unwelcome physical, verbal, or non-verbal conduct of a sexual nature.

This often leads to the feeling of intimidation, discrimination, and humiliation, and at worst it affects the victims both emotionally and mentally. The use of the word “gender” in the term “gender harassment” helps to broaden the understanding that harassment is not limited to a particular gender, rather it can affect all genders equally. While it is certain that women have historically faced higher rates of harassment and discrimination based on gender, it is important to recognize that individuals of all genders can be subjected to gender-based mistreatment.

Online gender harassment

Online gender harassment can be defined as a person receiving sexual threats, being coerced to participate in sexual behavior online, or being blackmailed with sexual content. It refers specifically to acts of harassment and discrimination based on gender that occur in the digital realm, such as through social media platforms, online forums, email, instant messaging, and other online communication channels.

Revenge Porn

Revenge porn refers to “revealing or sexually explicit images or videos of a person posted on the internet, typically by a former sexual partner, without the consent of the subject and in order to cause them distress or embarrassment." Mary Anne Frank (Law professor at the University of Miami) has remarked that ***“Revenge porn is a misnomer, instead, ‘non-consensual pornography' should be the appropriate term used"***.The driving factors behind such acts are couples' fantasies of filming themselves or a manipulative partner coercing the other to participate. However, current partners may also engage in revenge porn with the goal of regaining control or manipulating the other person to stay in the relationship. Perpetrators sometimes not only upload videos or images on porn websites but also include personal information about the subject, such as their full name, address, social media profiles, phone numbers, and more.

Revenge pornography lacks official statistics in India due to legal provision gaps, however, cases of online sharing of obscenity and nudity content increased by **104%** from 2012-2014 as reported by the National Crime Record Bureau. A Cyber & Law Foundation survey found that **27%** of Indian internet users aged 13 to 45 have been victims of such crimes. Additionally, such acts need not necessarily be the means of revenge but can rather be for profit. For example, the changing rooms within shops might harbor hidden cameras. For instance, following Union HRD minister Smriti Irani's discovery of a CCTV camera in the trial room of Fabindia in Goa, the Bombay High Court ordered the company to take drastic steps, including the permanent cancellation of their licenses.

Is banning porn a solution to revenge porn?

The Indian government has made multiple attempts to ban porn websites, blocking 800 in 2015, 827 in 2018, and an additional 67 in 2021, yet VPNs and other resources continue to circumvent these restrictions. Why are the governments of most countries failing to effectively ban pornography and curb other online crimes?

1. Porn is readily available on the web, just a search away on the internet. Since it is accessible globally, even if the government decides to ban it, they can only block a few hundred servers, leaving thousands of others still available on the internet.
2. Banning porn can be a failed attempt unless the government decides to invest substantial financial resources each year to maintain an up-to-date web content filtering system.
3. According to Pavan Duggal (cyber law expert), banning porn can stimulate curiosity among internet users and can act as a catalyst to increase traffic on blocked websites. More concerning is its fruitless nature as proxy servers allow individuals to access blocked sites outside India (as watching porn is not illegal in many countries).

4. Even if specific websites are banned, individuals can still access and download pornographic content through alternative means. For instance, BitTorrent technology allows users to download content, including porn, through peer-to-peer networks. Similarly, peer-to-peer networks like eMule and Bulletin Boards can be utilized for downloading and sharing files, including explicit material. This highlights the fact that banning websites alone may not effectively prevent access to pornographic content, as alternative channels and technologies exist for users to acquire such material.
5. Banning pornography can potentially raise concerns regarding the right to privacy and personal autonomy, which are protected under Article 21 of the Indian Constitution. A complete ban on pornography could be viewed as an infringement on an individual's right to access and consume legal adult content in the privacy of their own space.
6. Due to the significant role of pornography as a driving force behind e-commerce, most governments refrain from banning it. Most governments' (including India) action on this issue is to ban child pornography to protect the welfare of children.

A study conducted by UCLA researchers found that when comparing law-abiding men to the group of convicted rapists and child sex abusers, the latter group recalled consuming less pornography throughout their lives[1]. This indicates that there may not be a direct causal link between consuming pornography and engaging in sexual offenses. The solution to online gender offenses may not be banning porn but inculcating strong laws based on the ethics and morals of the country.

Sextortion

Sextortion refers to a form of online blackmail where an individual or group threatens to distribute explicit or compromising material, often sexual in nature unless a demand is met. Sextortion commonly begins with the perpetrator establishing contact with the victim, often through social media, dating platforms, or email. They may gain the victim's trust or trick them into sharing explicit content willingly. Once the perpetrator possesses compromising material, they use it as leverage to demand money, further explicit material, or other favors from the victim, under the threat of releasing the content to the public, friends, family, or colleagues. In India, the sextortion racket has reached alarming proportions, with more than 500 cases being reported every day. Shockingly, less than 0.5% of these cases are officially registered as FIRs (First Information Reports), indicating a significant underreporting of the crime. According to statements from Rajasthan police officers, they claim the entire population is involved in the sextortion racket. India was also given the title of the sextortion capital of the world in 2022 by various news reporters. The majority of the masterminds behind this

[1] UCLA

Sextortion crime are either individuals engaged in other criminal activities or currently unemployed individuals. Their primary targets are women, elderly men, business people, and young boys. In 2021, the Ghatkopar police uncovered a sextortion racket where the targets were businessmen. The UK's Revenge Porn Helpline revealed it received 1124 reports of sextortion in 2022, with nearly nine in ten (88%) cases involving male victims. In 2022, FBI statistics revealed over 7,000 reports of online sextortion of minors, impacting at least 3,000 victims, mostly boys. Many countries have addressed sextortion effectively. For example, in the United States the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) have specialized units to investigate and prosecute these cases, Philippines introduced the Anti-Photo and Video Voyeurism Act, making sextortion illegal. Furthermore, in Australia the government supports initiatives like the "ThinkUKnow" program, educating young people, parents, and teachers about online safety.

Other online harassment:

Cyberbullying: Cyberbullying refers to the act of using various digital communication technologies such as social media platforms to deliberately and repeatedly harass, intimidate and harm someone. Perpetrators of cyberbullying often hide behind anonymous or fake accounts making it difficult to find them. Examples of cyberbullying behavior include:

1. **Harassing messages:** Sending repeated abusive or threatening messages, emails, or comments to the victims, often using derogatory language.
2. **Spreading rumors:** Sharing false or malicious information about the victim with the intention of damaging their reputation or causing social harm.
3. **Online impersonation:** Creating fake profiles or accounts on social media platforms to humiliate the victims. This often includes pretending to be the victim on those platforms.
4. **Public humiliation:** Posting or sharing embarrassing, humiliating, or sexual photos, videos, or personal information of someone without their consent with the aim to shame or ridicule them.

Cyberstalking: Cyberstalking involves repeated monitoring of victims' online activities, or using spyware or hacking techniques to gain unauthorized access to the personal information of victims.

Doxing and exposing personal information: Revealing someone’s personal information such as their real name, address, or contact details, with the intention of inciting harassment or harm based on their gender.

Parasite Porn/ Deep Fake pornography: This practice involves using editing technology to superimpose faces to explicit or pornographic material without the individual's consent. It typically involves stealing photos from social media platforms or other sources and using sophisticated algorithms to replace the original person's face with someone else's.

Morph porn: Similar to parasite porn, this practice involves editing technology where the victim's face is copied, cropped, and pasted onto the body of another person who is engaging in explicit sexual acts.

Artificial Intelligence (AI) Powered Cyber Threats

Artificial Intelligence (AI) has become a powerful tool in our lives but it has the potential to manipulate us. Unfortunately, cybercriminals are now using AI to aid in their illegal activities online. Understanding AI's capacity to deceive and empower cybercriminals is pivotal in comprehending the evolving landscape of digital threats and devising effective strategies to safeguard our digital identities. Artificial intelligence (AI) has the potential to make online harassment, including revenge porn and sextortion.

AI-powered Cyberattacks:

AI-powered password hacking: Cybercriminals are using machine learning (ML) and AI to enhance their password-guessing algorithms, analyzing extensive datasets to generate various password variations and improve their cracking techniques. By employing such techniques, cybercriminals can intrude into individuals' private chats and access their images, subsequently exploiting this information for illicit purposes, such as engaging in sextortion.

Anonymity and Impersonation: AI-powered tools can facilitate anonymous communication and impersonation, allowing harassers to hide their identities and harass victims without fear of being identified. This makes it difficult to trace the harasser.

Deep Fakes: AI can generate realistic fake images, videos, and text, making it easier for perpetrators to create and share explicit or compromising content without the victim's knowledge or consent. These deepfakes can be used to carry out revenge porn. In September 2019, Deeptrace, an AI firm, discovered a staggering 15,000 deepfake videos online, with a remarkable 96% being of pornographic nature, and an astonishing 99% of those replacing the faces of female celebrities with those of pornographic actors.

Voice cloning: Voice cloning technology enables the creation of a digital replica of an individual's distinct voice, capturing speech patterns, accents, voice inflections, and even breathing, all by training an algorithm with a mere three-second audio clip from the person. According to a survey conducted by McAfee, 47% of Indians have encountered AI-generated voice scams, where fraudsters use advanced technology to fake kidnappings and extort money from unsuspecting individuals.

Impacts on victims and society:

Emotional and psychological harm: Victims of sextortion and revenge porn often experience significant emotional distress, humiliation, shame, and anxiety. Their personal lives and relationships may be negatively affected, leading to feelings of depression and even suicidal ideation. Out of all the people surveyed, nearly 7.5% of females, while only 2.3% of males, expressed that they seriously

thought about attempting suicide within the past year[2]. Surprisingly, offenders themselves are 1.7 times more inclined to commit suicide[3].

Betrayal trauma and PTSD: The violation of trust and privacy can have long-lasting psychological consequences which can also result in an inability to develop intimate relationships. Violations of trust, as seen in sextortion and revenge porn cases, can be considered a form of betrayal trauma. Betrayal trauma theory suggests that breaches of trust by close individuals or trusted entities can lead to significant emotional and psychological distress. Victims of sextortion and revenge porn may experience symptoms similar to post-traumatic stress disorder (PTSD). It can trigger symptoms such as flashbacks, nightmares, hypervigilance, avoidance of triggers, and emotional numbing. In a study conducted in Sweden, in 2019, it was found that adolescents engaged in cyberbullying, whether as victims or perpetrators, faced an elevated risk of experiencing symptoms associated with depression and anxiety, along with lower levels of overall well-being[4].

Shame, humiliation, and self-worth: The public humiliation and shame associated with having intimate images or videos shared without consent can significantly impact a person's self-esteem and self-worth. Victims may internalize the blame, experience self-loathing, and struggle with feelings of worthlessness, leading to depression, anxiety, and other psychological difficulties. Many times children below 18 years fall prey to such acts because of their curiosity or some filmy revenge theory. But according to one research, 19% of students who have been cyberbullied say that the experience negatively affected their feelings about themselves[5]. Therefore, they tend to hurt others. Nirali Bhatia, cyberpsychologist and founder of CyberBAAP, articulates a standpoint of the government official that no victim of cybercrime harassment wants to seek legal help because of the fear of the consequences they will face from society[6].

Economic Consequences: Sextortion and revenge porn can have economic repercussions on both individual victims and society. For victims, the aftermath may include loss of employment, damaged professional reputation, or the need for costly legal interventions. Additionally, society as a whole bears the burden of healthcare costs associated with treating the mental health consequences faced by victims.

---

2 https://bmcpsychiatry.biomedcentral.com/articles/10.1186/s12888-022-04238-x#:~:text=Nearly%207.5%25%20females%20compared%20to,did%20not%20 experience%20 cyberbullying%20 victimization.

3 https://www.stopbullying.gov/

4 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6981789/

5 https://nces.ed.gov/pubs2017/2017064.pdf

6 https://openthemagazine.com/cover-stories/the-trail-of-trauma/

Perpetuation of Gender-based violence: According to various reports and research in India, 4 in 10 men and women in India fall prey to online harassment through various social media platforms. The recent "State of the World's Girls Report," a comprehensive global survey conducted by Plan International, a UK-based humanitarian organization, has unveiled that girls and young women constitute a prominent demographic facing a high prevalence of online violence and abuse. Spanning 22 countries, including India, Brazil, Nigeria, Spain, Australia, Japan, Thailand, and the United States, the survey encompassed the perspectives of 14,000 women aged 15-25, shedding light on this pressing issue[7]. Sextortion and revenge porn contribute to the objectification of individuals, primarily targeting women. This can reinforce gender stereotypes, and undermine efforts towards achieving gender equity.

Normalizing Harmful Behavior: The widespread occurrence and acceptance of sextortion and revenge porn can normalize harmful behaviors and attitudes toward consent, privacy, and respect. It can contribute to a culture where non-consensual sharing of explicit content is seen as acceptable, reinforcing a negative cycle that perpetuates online harassment and exploitation.

Analyzing the existing Indian legal framework that deals with online gender harassment

In India, unfortunately, there is no specific law that deals with sextortion and revenge porn. These provisions may not include the terms ‘revenge porn’ or ‘sextortion’ thoroughly but cover some aspects of it.

Sections of the Indian Penal Code:

Section 292 and Section 292A: According to section 292, an object including books, pamphlets, papers, writings, drawings, representations, paintings, figures, or any other object, is deemed obscene if it is lascivious or appeals to prurient interest[8]. Section 292A prohibits the sale, distribution, or exhibition of obscene books, pamphlets, etc[9]. Additionally, if the object, or any of its distinct items in the case of multiple items, has an effect that tends to deprave and corrupt individuals, who are likely to read, see or hear its content, it is considered obscene. Further, it outlines the various actions that are considered offenses under this section and also specifies the punishment for such offenses. However, there are certain exceptions like objects that represent public good, science, literature, etc are not considered obscene in these sections.

[7] The Indian Express
[8] Section 292
[9] Section 292A

***Analysis*:**

1. Sections 292 and 292A primarily focus on the sale, distribution, and exhibition of obscene material without specifically addressing online gender harassment which makes it challenging to apply these sections effectively to tackle online gender harassment.
2. Section 292 in its definition primarily targets physical objects like books, pamphlets, etc which limits its scope to physical objects only. **To address online gender harassment, the legislation should adequately cover the harassment occurring through digital mediums, social media platforms, messaging apps, and other online spaces. Section 292 should include what constitutes obscenity on online platforms covering various online harassment acts including revenge porn, and sextortion with proper definitions to widen its scope.**
3. Additionally, the language of section 292A should be expanded to encompass actions such as 'sharing on online platforms', as current terminology implies 'physical distribution'.

Section 354: Section 354 of the Indian Penal Code (IPC) deals with the offense of 'assault' or 'criminal force' on women with the intent to outrage her modesty[10]. It aims to protect the dignity of women by penalizing individuals who assault or use criminal force against a woman with the knowledge that such an act is likely to outrage their modesty.

Analysis:

1. It is visible that this section primarily aims to provide protection to only 'women'. It makes it clear that this provision does not encompass the spectrum of genders, making it inefficient to curb online gender harassment.
2. Section 354 addresses two distinct types of acts namely 'assault' and the use of 'criminal force'. Assault refers to any act that causes apprehension of physical attack, and criminal force refers to the use of force that causes physical harm. Due to its exclusive focus on physical acts, section 354 of the IPC is inadequate in addressing the issue of online gender harassment.
3. While this section can be applied to certain cases of online gender harassment such as cyberbullying, it may not cover offenses like sextortion and revenge porn.
4. To specifically address online harassment the definition should be expanded to explicitly include acts committed through electronic means. Also, the offenses through online mediums including sextortion and revenge porn should be clearly defined.

Section 354A: Section 354A of the Indian Penal Code addresses the offense of sexual harassment and prescribes punishments for such acts[11]. According to sub-section (1) of section 354A, a man can be charged with the offense of sexual harassment if he commits any of the following acts:

[10] Section 354
[11] Section 354A

(i) physical contact and advances involving unwelcome and explicit sexual overtures.
(ii) demanding or requesting sexual favors.
(iii) showing pornography against the will of the woman.
(iv) making sexually colored remarks.
Further, it specifies punishments for such offenses.

Analysis:

1. While Section 354A recognizes certain forms of sexual harassment, it may not be sufficient to curb online gender harassment. **The definition of sexual harassment within section 354A could be expanded to cover a wider range of behaviors, including those specific to online platforms. This may include online harassing acts like sextortion and revenge porn.**
2. Also, it seems to be a women-centric provision, therefore rather than being gender specific it should be neutral.

Section 354B: Section 354B of IPC states that if the man assaults or uses criminal force against a woman, or abets such an act, with the intention of disrobing her or compelling her to be naked the act is considered a serious violation of women's dignity and privacy[12].

Analysis: While section 354B of the IPC prohibits physically compelling women to be naked, it does not specifically address acts of coercing or compelling women to be naked in videos or on other online platforms. In addition, online harassment involves unique dynamics and challenges which should be addressed appropriately in this section.

Section 354C: Section 354C refers to any man who watches or captures the image of a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed, either by a perpetrator or by any other person, shall be subject to punishment[13]. Dissemination of such images is also considered an offense under this section. In this section 'private act' refers to an act of watching carried out in a place that would reasonably be expected to provide privacy, where the victim's genitals, posterior, or breast are exposed or covered only in undergarments, or where the victim is using the lavatory or the victim is engaged in a sexual act. This act aims to address the invasion of women's privacy by penalizing acts of voyeurism. In Udupi, Karnataka, three Muslim girls from a college were arrested for filming Hindu female students in the restrooms, an act punishable under Section 354C for invasion of privacy through voyeurism.

Analysis:

1. While section 354C of the IPC addresses the offense of voyeurism and provides penalties for watching, capturing, or disseminating private images of women, it may not be sufficient to tackle

[12] Section 354B
[13] Section 354C

the broader issue of online gender harassment. Online gender harassment encompasses various forms of harassment, including but not limited to voyeurism.

2. **In light of the Udupi case, understanding the significance of gender-neutral provisions becomes essential in addressing privacy violations and ensuring equal protection under the law.**

Section 354D: Section 354D is a specific section of the Indian Penal Code that deals with the offense of stalking[14]. It was introduced in 2013 as a part of the Criminal Law (Amendment) Act, which aims to strengthen laws related to sexual offenses in India. It provides the definition of stalking and outlines the action that constitutes the offense. Stalking is defined as the following actions performed by a man towards a woman.

(i) following a woman and repeatedly contacting or attempting to contact her in order to foster personal interaction, even after the woman has clearly indicated disinterest.

(ii) monitoring women's use of the internet, email, or any other form of electronic communication.

The interpretation and the application of section 354D may vary depending on the specific jurisdiction within India. There are also exceptions listed in this provision.

Analysis:

1. Section 354D deals with stalking, however, it does not cover the full range of online gender harassment issues. Along with stalking, online gender harassment encompass various forms such as cyberbullying, defamation, revenge porn, sextortion, etc. **Also, it should explicitly define what stalking constitutes on online platforms.**
2. The current section only addresses offenses committed by men against women. While it acknowledges the prevalent gender dynamics in cases of stalking. **It does not explicitly cover instances where men are victims, or cases involving non-binary or transgender individuals.**
3. The section does not provide a clear definition of what constitutes 'monitoring' of women's online activities. This lack of clarity may lead to different interpretations and inconsistencies in the application.

Section 383: Section 383 of the Indian Penal Code defines the offense of extortion[15]. Extortion occurs when a person intentionally puts another person in fear of injury, either to themselves or someone else, and as a result, dishonestly induces the person in fear to deliver property, valuable security, or anything signed or sealed that can be converted into a valuable security to any person. The section provides

[14] Section 354D
[15] Section 383

several illustrations to help understand the concept of extortion. The specific application and interpretation of the law may vary depending on the jurisdiction and the circumstances of each case.

Analysis:

1. While section 383 of the IPC encompasses extortion-related offenses, its failure to encompass sextortion or acknowledge the exchange of sexual favors undermines its effectiveness in addressing online gender harassment.
2. In addition, it should explicitly prohibit any sharing, posting, or blackmailing of nonconsensual pornography or any online activity that outrages one's modesty. Clear definitions of sextortion and revenge porn along with illustrations will help to interpret this section effectively.

Section 499: Section 499 of the Indian Penal Code deals with the offense of defamation[16]. It states that whoever, by words spoken or intended to be read, signs, or visible representation, makes or publishes any imputation concerning any person with the harm or knowing or having reason to believe that such imputation will harm the reputation of that person, commits defamation. The section further provides an explanation and the exceptions to defamation.

Analysis:

1. Section 499 of the Indian Penal Code primarily focuses on the harm caused to a person's reputation. However, online gender harassment often involves non-consensual sharing of explicit content, threats, blackmail, and other forms of harassment that goes beyond reputation damage. Considering that one's reputation can be defamed on digital platforms, this section does not explicitly address electronic communication, making it less equipped to handle such cases effectively.
2. Section 499 should also include various forms of online harassment with proper definitions to broaden the scope of this section.
3. **Furthermore, it is necessary to include the term 'sharing on online platforms' alongside the term 'publish' in order to explicitly address and combat online gender harassment.**

Section 503: Section 503 deals with the offense of criminal intimidation[17]. According to section 503 of the Indian Penal Code, whoever intimidates or threatens another person with the intention to cause that person to fear for their safety, or their property, commits the offense of criminal intimidation. This intimidation can be done through spoken or written messages, signs, gestures, or any other visible representation.

Analysis:

---

[16] Section 499

[17] Section 503

1. Section 503 does not explicitly mention online gender harassment or any of its forms. It should inculcate intimidation through digital mediums such as messaging apps, websites, calls, etc. Online offenses such as sextortion and revenge porn take place on online platforms. These offenses use explicit images, videos, or personal information for coercion or harassment, which may not be fully addressed under section 503.
2. **To tackle online gender harassment section 503 should widen its scope thereby including various forms of online intimidation with proper definitions and illustrations.**

Section 507: Section 507 of the Indian Penal Code deals with the offense of criminal intimidation by anonymous communication[18]. The offense of criminal intimidation by anonymous communication occurs when a person engages in an act of criminal intimidation through a communication where their identity is concealed. This could involve sending threatening messages, making intimidating phone calls, or any form of communication that induces fear in a victim.

Analysis:

1. Though section 507 of the Indian Penal Code deals with some of the aspects of online gender harassment i.e. criminal intimidation by anonymous communication, it does not effectively address what anonymous communication means when it comes to digital harassment. Criminal intimidation through anonymity is a very general term, often online harassment involves an anonymous person making it difficult to find the harasser.
2. **Anonymity in the online realm can include the creation of fake profiles and accounts, the use of Virtual Private Networks (VPN), and encrypted messaging apps making it challenging for the authorities to intercept or trace the content. Section 507 should include all these possible mediums keeping in mind the broader aspects of it.**

Information Technology (Amendment) Act 2008:

While the Information Technology Act 2008 (amended) of India does not specifically mention stalking or online harassment, however, this issue is dealt with as an 'intrusion onto the privacy of individuals in the act.

Section 66A: Section 66A of the IT Act 2000 was an amendment introduced in 2008. However, it was struck down as unconstitutional by the supreme court of India in 2015. What makes it worth mentioning here is its attempt to address prevailing cyber crimes. Prior to its repeal, section 66A criminalized the sending of offensive or menacing messages through a computer resource or communication device. It stated that any person who sent such messages, which were known to be false, deceptive, or cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal

[18] Section 507

intimidation, or enmity could be punished with imprisonment for a term that could extend up to three years along with fine. Section 66A drew significant criticism for its broad and vague language, leading to its misuse and violation of freedom of speech and expression. The Supreme Court in its judgment in Shreya Singal v. Union of India, declared section 66A unconstitutional, stating that it violated the fundamental right to freedom of speech and expression guaranteed by the Indian Constitution.

Analysis:

1. Considering the rise of cyber crimes in India, it is vital to introduce laws that deal with specific cybercrimes such as cyberstalking, revenge porn, sextortion, etc. There should be efforts to introduce new laws that clearly define what constitutes online harassment, including behavior like stalking, cyberbullying, revenge porn, and doxing.
2. Specificity in language can help prevent ambiguity and ensure that the law targets actual instances of harassment. By focusing on precise and well-defined offenses, the law can avoid vagueness and overreach.
3. **It is crucial to strike a balance between protecting individuals from online harassment and safeguarding freedom of speech (a fundamental right under Article 19(1)(a) of the Indian Constitution). This can be done through a clear demonstration of intent to harm or harass. This can help ensure that mere expressions of opinions or criticism do not fall within the purview of the offense.**
4. The focus should be on actions that are intentionally and maliciously harmful rather than dissenting views. Illustrations for effective implementations:
    a. In the case of revenge porn- the law can require evidence of an individual knowingly and intentionally sharing explicit material with the intention to harm, shame, or defame the victim. The provision could specify that the offense of revenge porn applies when someone knowingly distributes explicit images or videos of another person without their consent with the clear intention to cause harm or blackmail.
    b. In the case of sextortion, the provision could state that sextortion is applicable when an individual uses threats, coercion, or blackmail to obtain explicit images or engage in sexual activities against someone's will, with the clear intent to exploit them or gain something in value that may be sexual favors or property.

Section 66C: Section 66C of the Information Technology Act, 2000 deals with the offense of identity theft in India. The offense of identity theft in this section is defined as ‘whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment for a term of up to one lakh rupees’. The purpose of this provision is to protect individuals from identity theft and unauthorized use of their digital identity or personal information.

Analysis:

1. Section 66C of the Information Technology Act, 2000 does not explicitly address identity theft in relation to online harassment or bullying. It should explicitly mention that using stolen or impersonated identities for the purpose of online harassment is an offense under this section. Also, online gender harassment including sexist remarks, misogynistic threats, etc using the profile of the victim is punishable and falls under the purview of online gender harassment.
2. **This section should also encompass various methods used by perpetrators to steal and misuse someone's identity. This can include monitoring the activities of victims through their passwords, gaining unauthorized access to their online accounts, commenting on someone's gender using that profile, etc.**
3. In addition, introduce provisions to prohibit the creation of fake accounts or profiles with the intent to impersonate someone else and engage in harassment or identity theft.

Section 66E: Section 66E of the Information Technology (IT) Act of India deals with the offense of capturing, transmitting, or publishing private images of a person without their consent. It specifically addresses the violation of privacy through the use of electronic and digital media. In this context, 'private area' refers to the naked or undergarment-clad genitals, pubic area, buttocks, or female breasts. The section defines key terms such as 'transmit', 'capture', 'publishes', and 'under circumstances violating privacy' to provide clarity and proper interpretation of the law.

Analysis:

1. Though this act deals with some aspects of online harassment, it does not address gender harassment. While it focuses on the transmission of explicit photos, it does not mention the prohibition of blackmailing the victims through these photos or videos.
2. The provision should include other online harassment acts like cyberbullying, and sextortion, and then can it effectively address online gender harassment.

Section 67A: Section 67 deals with the provision related to the publication or transmission of material containing sexually explicit acts or conduct in electronic form. This provision aims to address content that is sexually explicit and imposes penalties for those involved in its publication or transmission.

Analysis:

1. Considering the unique challenges and the diversity of online harassment, this provision does not provide detailed criteria for what constitutes 'sexually explicit material'. The lack of specific definitions can lead to ambiguity and challenges in interpreting and applying the law consistently.
2. The section should also explore other areas where these explicit images and videos can be used to harass other people, like cyberbullying, sextortion, revenge porn, etc

Section 67B: Section 67B of the Information Technology (IT) Act of India addresses the punishment for publishing or transmitting material depicting children engaged in sexually explicit acts or conduct in electronic form.

Analysis: The study shows 59.2% of kids use smartphones for messaging, while only 10.1% of them utilize smartphones for online learning and education. Surprisingly, 37.8% of 10-year-olds have Facebook, 24.3% on Instagram. To effectively protect children from online harassment, this section should incorporate various online harassment acts like cyberbullying, sextortion, compelling children to be naked in photos or videos, etc.

POCSO (Protection OF Children From Sexual Offenses) Act, 2012

The POCSO Act refers to the Protection of Children from Sexual Offences Act, which is a law enacted in India. It was established in 2012 and provides legal protection for children under the age of 18 from various forms of sexual abuse, exploitation, and pornography. The act defines different types of sexual offenses against children, including penetrative and non-penetrative assault, sexual harassment, and the use of children for pornographic purposes.

Analysis:

1. To effectively tackle online sexual harassment against children the act should encompass a broader range of online harassment with its proper definition.
2. The act primarily focuses on punishment and prosecution after an offense has occurred. A more proactive approach could involve incorporating preventive measures, such as awareness campaigns, educational programs, and digital literacy initiatives. These efforts would empower children, parents, and educators to identify and respond to online gender harassment effectively.
3. While the act emphasizes the punishment for offenders, it may not adequately address the support and rehabilitation needs of victims. Establishing comprehensive victim support systems, including counseling services, helplines, and specialized courts, would ensure a holistic approach to addressing the impact of online gender harassment on children.

Indecent Representation of Women (Prohibition) Act, 2012

Another act that specifically deals with cybercrimes against women in India is the "Indecent Representation of Women (Prohibition) Act, of 2012".The act was enacted to address the issue of objectification, exploitation, and stereotyping of women in visual media, including advertisements, publications, films, television, and the Internet. Cyber law expert Pavan Duggal recommended that India needs dedicated legal provisions for protecting women in cyberspace, and data related to women needs to be specifically protected.

Analysis:

1. The act primarily focuses on regulating the representation of women in visual media such as advertisements, films, and television. It may not adequately cover other forms of online gender harassment, such as cyberbullying, online stalking, grooming, or dissemination of explicit content through social media platforms.
2. The act defines "indecent representation" but lacks specific guidelines or criteria to determine what constitutes indecent or derogatory representation. This ambiguity can lead to inconsistent interpretation and implementation of the law. Providing clearer definitions and guidelines would ensure more consistent enforcement.

The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013

The Sexual Harassment of Women at Workplace Act emphasizes the importance of creating a safe and respectful working environment for women. It establishes a clear framework for addressing and redressing complaints of sexual harassment, ensuring that victims have a platform to seek justice.

Analysis: As COVID emerged, a novel work culture known as "remote work" came into existence, and as times evolve, it becomes imperative to acknowledge the necessity of safeguarding workers' rights in the digital realm. It is suggested that the legal framework should be adapted to properly integrate work-from-home arrangements and protect working women from sexual harassment in cyberspace. Interpreting the term "dwelling place or house" in the POSH Act solely in relation to domestic help or servants would be narrow and restrictive. Instead, it advocates for a dynamic approach that broadens the definition of a "workplace" to include telework. Amid the COVID-19 pandemic in FY20, many companies reported an aggregate of 999 sexual harassment cases against women in India, as the #MeToo movement gained momentum, leading to increased awareness and employee activism. They were harassed by receiving hurtful messages, encountering discriminatory content, being trolled and shamed online, and facing incidents of impersonation and hacking. The following points should be taken into consideration while crafting a law that deals with the digital workplace.

1. It is vital to define key terms related to cyber crimes, such as hacking, unauthorized access, data breach, identity theft, online harassment, phishing, etc.
2. To make sure the acts work effectively it is important to clearly define the digital workplace to encompass any online or digital environment where work-related activities take place, including remote work settings.
3. Establish the responsibilities of employers to maintain secure digital work environments, including implementing appropriate security measures, providing cybersecurity training, and promptly addressing reported incidents.
4. Specify the procedures for reporting cyber crimes in the digital workplace, including confidential reporting channels and protection for whistleblowers.

5. Stringent punishment should be incorporated in the process of formulating such law and proper penalties should be prescribed.

Notable Case Studies of Revenge Porn and Sextortion in India

The case of State of West Bengal v. Animesh Box[19] i:

The case of the State of West Bengal v. Animesh Boxi serves as a notable case study in the context of revenge porn. This case is believed to be the first ever case that deals with revenge porn.

Background: In the case of State of West Bengal v. Animesh Boxi, which took place in March 2018, the accused, Animesh Boxi, uploaded private and objectionable pictures of a girl on the internet without her consent. The accused and the victim had been in an intimate relationship, and the explicit images were obtained by the accused under the false promise of marriage. After the victim broke off the relationship, the accused sought revenge by uploading the images and videos on pornographic sites, using both the victim's and her father's names.

Verdict: The Sessions court in Tamluk, West Bengal, pronounced the judgment in the case. Animesh Boxi was found guilty and sentenced to five years of imprisonment, along with a fine of Rs. 9,000. The accused was convicted under various sections of the Indian Penal Code, including Sections 354, 354A, 354C, and 509, which pertain to sexual harassment and outraging the modesty of a woman. Additionally, the accused was convicted under Sections 66E, 66C, 67, and 67A of the Information Technology Act, which deal with the unauthorized capture, publication, or transmission of explicit content.

Learnings:

1. Firstly, it emphasizes the importance of ensuring that laws encompass digital offenses and adequately protect individuals from cybercrimes, including revenge porn.
2. This case is special and sets an example because of the court's directive to treat the victim as a rape survivor and provide compensation. It acknowledges the harm caused to the victim and signifies the importance of addressing the emotional and psychological impact of revenge porn. This sends a powerful message about the legal system's responsibility to protect and support victims.

Mangalore kidnapping and sextortion case[20]:

Background: In this case, a gang of eight individuals came across a young couple, both medical students, outside a restaurant on the outskirts of Mangalore late at night. The gang kidnapped the couple, forced them into sexual acts, and recorded the scenes with the intention of blackmailing and extorting money from them. The couple was subjected to multiple nights of captivity and abuse.

---

[19] C.R.M. No. 11806 of 2017, GR/1587/2017.

[20] Mangalore Sextortion Case

Verdict: Following a police raid on the gang's hideout, the male student was rescued from captivity. All eight members of the gang were arrested. The accused faced charges of kidnapping, assault, blackmail, and extortion. It was revealed that some of the gang members had prior criminal records, including cases of armed robbery. The evidence, including the mobile phones of the accused, was seized for investigation purposes.

Learnings:

It demonstrates that apart from women, other genders including male and non-binary people are also victims of such heinous acts.

Legislation From Across The Globe:

By examining the innovative approaches, successful policies, and effective frameworks implemented elsewhere, India can uncover inspiration to address its own unique challenges.

California:

California's laws related to sextortion:

In California, sextortion cases are typically prosecuted under extortion and child pornography laws. Cases involving minors may also lead to child pornography charges due to the illegal exchange or possession of explicit images of minors. To combat sextortion, California has established dedicated task forces and units within law enforcement agencies. The state also emphasizes raising awareness and educating the public about sextortion prevention and response. This includes implementing online safety programs in schools, conducting awareness campaigns, and providing resources to help individuals recognize signs of sextortion and report incidents to the appropriate authorities.

California's laws related to revenge porn:

Under California law, revenge porn is a criminal offense. Penal Code Section 647(j)(4) defines revenge porn as the distribution of intimate images of another person without their consent, with the intent to cause distress or harm. This includes sharing explicit photos or videos of someone without their permission, typically after a relationship has ended[21].

Victims of revenge porn in California have legal recourse to seek justice. The state allows individuals to file civil lawsuits against the person responsible for distributing their intimate images without consent. Additionally, victims can seek a restraining order to prevent further dissemination of the material.

United Kingdom:

United Kingdom's laws related to sextortion:

In the United Kingdom, sextortion cases are typically addressed under the Sexual Offences Act 2003 and the Communications Act 2003. The Sexual Offences Act 2003 includes provisions related to

[21] California on revenge porn

blackmail (Sections 33 to 35), which can apply to sextortion cases. Blackmail involves making unwarranted demands, including demands for money or valuable consideration, with the threat of disclosing explicit material. The offense is committed when the intention is to cause distress, gain something, or influence the victim's actions.

The Communications Act 2003, specifically Section 127, covers offenses related to the sending of grossly offensive, indecent, obscene, or menacing messages, including those involved in sextortion. It is an offense to send such messages with the intent to cause distress or anxiety to the recipient.

United Kingdom's laws related to revenge porn:

The Criminal Justice and Courts Act 2015 introduced the offense of disclosing private sexual photographs and films with the intent to cause distress. The Sexual Offences Act 2003 (Amendment), also implemented in 2015, expanded existing legislation to cover the offense of disclosing private sexual photographs and films with the intent to cause distress. This amendment extended the application of revenge porn laws to encompass both consensual and non-consensual intimate images. Defamation laws in the UK protect individuals from false statements that harm their reputations.

Challenges in the legal framework:

1. India does not have dedicated and comprehensive legislation specifically addressing sextortion and revenge porn. The absence of clear definitions and specific provisions related to these offenses can create ambiguity and hinder effective legal recourse.
2. Another challenge in India is that different interpretations of the law can result in varying judgments and punishments in sextortion and revenge porn cases.
3. India's laws focus on protecting women but often neglect the recognition of other genders or gender neutrality in their provision.
4. In India, there is a lack of provisions that empower victims to request the removal of their explicit pictures from websites, which can undermine the trust of victims in the legal system.
5. While the IT Act 2000 addresses certain sexual offenses related to cybercrime, it fails to adequately encompass the evolving nature of cybersexual crimes.
6. Awareness about sextortion and revenge porn among the general public, as well as law enforcement agencies, may be relatively low. This lack of awareness can result in underreporting of incidents.
7. Sextortion and revenge porn cases often cross international borders, making it difficult to track and hold perpetrators accountable due to jurisdictional challenges.
8. Victims of sextortion and revenge porn may feel ashamed, stigmatized, and afraid of retaliation, which can discourage them from reporting incidents. This reluctance hampers the identification and prosecution of perpetrators and the support offered to victims.

9. The Indian legal system's case backlog contributes to delays in resolving sextortion and revenge porn cases, this can diminish the hopes of victims to seek justice.

Policy Recommendations:

1. It is strongly recommended to create a commission dedicated to tackling gender-based crimes in online spaces. Such a commission may be known as ***National Commission for Cybercrime*** or ***National Cybercrime Commission (NCC)***. This commission pledges and strives to deliver justice for all genders. The National Cybercrime Commission (NCC) may consist of a Chairperson, appointed by the central government for expertise in cybersecurity, along with five members selected for competence in diverse fields such as cybersecurity, legal and legislative matters, technology, women's empowerment, academia, social welfare, and law enforcement. Moreover, a Member Secretary may be chosen preferably for their knowledge of cybersecurity. Functions and responsibilities:

   1.1 . ***Investigation and Examination***: The NCC shall be able to investigate and examine all cybercrimes affecting women, men, and non-binary individuals ensuring their protection and safety in the digital space.

   1.2 ***Legal Intervention***: The NCC shall develop innovative mechanisms, such as a Cyber Lok Adalat, to facilitate the redressal and speedy disposal of cybercrime cases. NCC shall periodically review existing laws affecting all genders in cybersecurity and provide gender-neutral recommendations for amendments to enhance their protection and empowerment. Additionally, NCC shall look into complaints and take suo moto notice of matters relating to the deprivation of an individual's rights.

   1.3 ***Research and Special Studies***: The NCC shall conduct research and special studies on emerging cyber threats against all genders, identifying the challenges and proposing practical strategies for their elimination.

   1.4 ***Awareness and Education***: The NCC shall engage in awareness campaigns in Colleges, Universities, NGOs, etc to educate about online safety and the reporting of cybercrime. Drawing inspiration from organizations like the Association of Media Women in Kenya (AMWIK), it is recommended that the National Cybercrime Commission (NCC) should provide digital security training for all genders to empower individuals in effectively countering online harassment and safeguarding their digital presence.

   1.5 ***Collaboration and Advocacy***: The NCC shall collaborate with relevant authorities, law enforcement agencies, and other stakeholders to advocate for stringent laws and policies aimed at curbing cybercrimes.

1.6 ***Funding Support***: The NCC will provide financial support to individuals facing cybercrimes, to ensure their access to legal recourse and representation.

1.7 ***Reporting and Evaluation***: The NCC shall prepare periodic reports on the prevalence and nature of cybercrimes, assessing the progress made in addressing these issues.

2. Considering the rise of cyber crimes in India, it is recommended to introduce laws that deal with specific cybercrimes such as cyberstalking, revenge porn, sextortion, etc. It is suggested to focus on well-defining laws to avoid vagueness and better serve their intended purpose.
3. To avoid the challenge of different interpretations of the law and varying judgments, it is suggested to promote consistency in the interpretation of laws to ensure uniform judgments and punishments in sextortion and revenge porn cases in India. This can be achieved through the establishment of specific guidelines, training programs for judges and legal professionals.
4. The state should develop laws that are gender-neutral, ensuring that individuals of all genders, including men and non-binary people, can seek provisions under the same legal framework.
5. It is suggested that acknowledging the rights of victims over their selfies and extending copyright protection to revenge porn and sextortion, can empower victims to issue takedown notices for the removal of their explicit images from the internet.
6. India should create a dedicated service like the UK's "Revenge Porn Helpline" which will work closely with online platforms to ensure the swift removal of explicit content of victims.
7. The 'right to be forgotten' (which mandates the erasure of data when it is no longer necessary or consent is revoked by the individual) recognized under the GDPR (Europe's General Data Protection Regulation), should be incorporated into Indian law to protect digital privacy, as it is currently not recognized.
8. Considering the evolving nature of the internet and cybercrimes, it is advised to propose amendments with proper definitions that align with the characteristics of contemporary crimes.
9. A balance be struck between safeguarding freedom of speech (a fundamental right under article 19(1)(a) of the Indian Constitution) and protecting individuals from online harassment. This can be done by following the digital footprint or online pattern of an individual on the internet to harass the victim. The focus should be on the repetitive actions of an individual regarding the victim(s) that are intentionally and maliciously harmful rather.
10. To facilitate victim complaints, it is recommended to establish dedicated channels on social media platforms, such as a WhatsApp bot, to ensure ease of reporting. To prevent fraudulent claims, it is suggested that victims provide supporting evidence such as snapshots of messages.
11. To protect victims from any social harm or stigmatization, it is suggested to protect victims' confidentiality, their personal information should be kept confidential during the investigation.

12. Given the challenges faced by women as victims of Sextortion and other cybercrimes, including judgment and anxiety that may discourage them from reporting the crime, it is imperative to suggest legislation to require the assignment of female officers to handle such cases.
13. To tackle the challenges posed by sextortion and revenge porn across borders, India can utilize global forums like G20. India can use the global platform of G20 to work with other countries in creating a response mechanism that tackles cross-border issues, taking into account the different laws of each country involved. India can also participate in regional cybersecurity exercises and drills conducted by SCO (Shanghai Cooperation Organization) for gaining practical experience in coordinated responses to cyber threats.
14. India can learn from the UK's model of collaboration between different law enforcement agencies to effectively address sextortion and revenge porn. Establishing specialized units or task forces dedicated to investigating these crimes.
15. Indian legal system should address its significant case backlog to ensure timely resolution of sextortion and revenge porn cases. This can be achieved by establishing fast-track courts to specifically address online harassment and other cyber crimes, thereby ensuring prompt and efficient delivery of justice.
16. India should recognize cybercrime victims, including those impacted by revenge porn and sextortion, as rape victims and adopt California's approach to provide civil remedies and comprehensive victim services. These services encompass crisis counseling, legal advocacy, support groups, and referrals to relevant resources, facilitated by non-profit organizations like CALCASA and the California Victim Compensation Board, supporting victims in their recovery.
17. Spreading awareness about emerging cyber crimes through programs in schools, colleges, and workplaces can help people recognize the seriousness of these crimes and learn how to tackle them, paying particular attention to the psychological effects they can have.
18. By expanding the definition of the Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act, 2013 to encompass telework, effective measures can be implemented to combat online harassment in digital workspaces.
19. Incorporating strict penalties, such as 5-10 years of imprisonment and fines up to ₹ 25,000, can contribute to reducing the occurrence of the crime. Also, making sextortion and revenge porn cognizable offenses can help acknowledge their severity.

Conclusion

In conclusion, this research paper has made a sincere effort to address the challenges present in the Indian legal system concerning online harassment. By thoroughly examining the legal systems of various countries and incorporating the recommended changes, it is highly plausible that positive

transformations can be witnessed. Implementing these changes will not only reinforce the rights of victims but also position India as a model for enacting effective laws on online harassment. By prioritizing victim protection and adapting to the evolving digital landscape, India can pave the way for a safer and more inclusive online environment, setting an example for other nations to follow.

REFERENCES

- POCSO Act, 2012-Ministry of Women and Child Development https://wcd.nic.in/sites/default/files/POCSO%20Act%2C%202012.pdf
- Handbook on Sexual Harassment of Women at Workplace-Ministry of Women and Child Development https://wcd.nic.in/sites/default/files/Handbook%20on%20Sexual%20Harassment%20of%20Women%20at%20Workplace.pdf
- TheIndecentRepresentation-Lok Sabha Secretariat Intranet https://loksabhadocs.nic.in/Refinput/New_Reference_Notes/English/The_indecent_representation.pdf
- Information Technology Act 2000 - 2008 (amendment).pdf https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf
- Puneet Bhasin. "Legal Provisions And Steps To Report Online Harassment Against Women|ForbesIndia,"August30,2022. https://www.forbesindia.com/amp/article/brand-connect/legal-provisions-and-steps-to-report-online-harassment-against-women/79393/1
- Amrita Madhukalya. "Are Laws against Online Harassment Enough? | Deccan Herald," January 15, 2022. https://www.deccanherald.com/specials/sunday-spotlight/are-laws-against-online-harassment-enough-1071483.html.
- Chandrima Khare. "Laws Punishing Cyber Stalking and Online Harassment." IPleaders (blog), July 13, 2018. https://blog.ipleaders.in/cyber-stalking/.
- Jyoty Thakur. "Sextortion: An Emerging Crime Into The Gray Area Of Law." Legal Service India. https://www.legalserviceindia.com/legal/article-6707-sextortion-an-emerging-crime-into-the-gray-area-of-law.html
- "Revenge Porn Or Non-Consensual Pornography." India Law Offices LLP. https://www.indialawoffices.com/legal-articles/revenge-porn-or-non-consensual-pornography
- Harish Nair, Javed Anwar. "Five Reasons Why Porn Ban Won't Work" India Today, August 4, 2015. https://www.indiatoday.in/mail-today/story/five-reasons-why-porn-ban-wont-work-286248-2015-08-03.

- Samraddhi Shetty, Anirudh Narendra. "Of Sextortion, Laws, and What Victims of This Crime Can Do." The Hindu Businessline, April 27, 2018, sec. National. https://www.thehindubusinessline.com/news/national/of-sextortion-laws-and-what-victims-of-this-crime-can-do/article23726557.ece
- Apoorva Gaur. "Volume 1 & Issue 3 » UNDERSTANDING 'SEXTORTION & REVENGE-PORNS' AS NEW FACE OF CYBER CRIME: A NEED FOR REFORM IN INDIAN CYBER LAWS »." Law Audience Journal 1 (April 2019). https://www.lawaudience.com/understanding-sextortion-revenge-porns-as-new-face-of-cyber-crime-a-need-for-reform-in-indian-cyber-laws/
- Ullekh NP. "The Trail of Trauma - Open The Magazine," January 14, 2022. https://openthemagazine.com/cover-stories/the-trail-of-trauma/.
- Sehgal, Diganth Raj. "How to Take Legal Action against Sextortion." IPleaders (blog). https://blog.ipleaders.in/take-legal-action-sextortion/
- Dhananjay Mahapatra. "Need 'Right to Be Forgotten' to Fight Revenge Porn: HC - Times of India." The Times of India, November 24, 2020. https://timesofindia.indiatimes.com/india/hc-bats-for-victims-right-to-be-forgotten/articleshow/79378100.cms.
- Disha Chaudhari. "Analysing The Indecent Representation of Women (Prohibition) Bill 2012." Feminism in India, February 8, 2017. https://feminisminindia.com/2017/02/09/indecent-representation-women/
- Smita Pandey. "Cyber Laws And POCSO Act." Legal Service India. https://www.legalserviceindia.com/legal/article-4645-cyber-laws-and-pocso-act.html.
- Shreyaa Mohanty. "Cyber Crimes Against Women : What Do the Indian Laws Say? | ProBono India," May 6, 2020". https://probono-india.in/blog-detail.php?id=118.
- Rishab Chhabaria, Abhigyan Tripathi. "Prevention of Sexual Harassment at 'Online' Workplace – The Leaflet," June 4, 2020. https://theleaflet.in/prevention-of-sexual-harassment-at-online-workplace/.