FROM HARASSMENT TO HATE: THE LEGAL BATTLE AGAINST CYBER VIOLENCE ON WOMEN IN INDIA

Mansi Kaushik*

ABSTRACT

In ancient times, according to Hindu Scriptures, women were often depicted as "Goddesses" (Devi) and cherished as representations of prosperity. The Early Vedic Period was marked by women participating in many religious rituals and often considered as "Ardhangini" or "Better half" to their husbands. But from ancient times to modern times, crimes against women are increasing day by day. These crimes are not only limited to the physical world but also happen in the cyber world. Cybercrime against women is a growing global issue which involves various online crimes like forms of harassment, defamation, cyberstalking, identity theft, and many more crimes that impact the victim offensively. In India, the existing laws are not enough and are not capable of dealing with the growing issue of cybercrime, because of gaps in enforcement, lack of awareness among people and the evolving nature of technology, it needs to be stricter and more protective in nature for the victims. This paper consists of the various crimes against women in the cyber world, their impacts on the victim, and laws addressing cybercrime against women in India.

Keywords: Cyber Crime, Cyber Crime Against Women, Cyber Stalking, Cyber Bullying, Cyber Morphing.

INTRODUCTION

In today's world, the rapid growth of information and technology gives a platform to individuals for interaction and communication. This cyberspace gives a new path for easy access to education, employment and social empowerment; similarly, it also gives rise to some challenges, such as cybercrimes and cybersecurity. Among these challenges, women are targeted as the victims of online crimes such as cyberbullying, cyber stalking, online

*BA LLB (HONS.), FOURTH YEAR, SAGE UNIVERSITY, BHOPAL.

harassment, cyber pornography, voyeurism, trolling, and abusive emails from multiple IDs. These crimes violate the women's privacy and dignity.

Therefore, some laws enacted in India that address cybercrime against women, such as the Information Technology Act, 2000 and relevant provisions of Bharatiya Nyaya Sanhita, 2023. Also, Judicial Interpretation and landmark cases played an important role in shaping legal frameworks.

MEANING OF CYBER CRIME

Cybercrime is a type of illegal activity that uses a computer, computer network, the internet or any electronic or network device for the commission of a crime in the cyber world. Cybercrime is conducted by any individual or organisation with the purpose of gaining profit or causing damage to any individual or organisation.[1] There are three categories of cybercrime:

1. against an individual (man, woman, organisation)
2. against property
3. against the government (which is known as cyber terrorism)[2]

MEANING OF CYBER CRIME AGAINST WOMEN

Cybercrime against women falls under the very first category of cybercrime, that is, cybercrime against individuals. Cybercrime against women involves criminal activity by use of a computer, network or network device to commit a crime targeting women with the intention to cause harm. (harm can be either physical, mental or financial)

TYPES OF CYBER CRIMES AGAINST WOMEN

Cyberbullying: Cyberbullying refers to causing harm, insult, harassment, humiliation, abuse, or embarrassment to a woman by posting, sending, or sharing harmful, false, or negative content about her through the use of electronic devices, such as smartphones, computers, and internet platforms like social media and dating apps.

Cyber stalking: Cyber stalking is monitoring a woman on social media platforms and repeatedly sending them threats, abusive or obscene messages by any electronic means

[1] 'Cyber Crime: Meaning, Types, and Examples' (Legal Service India, 2022)
[2] National Crime Records Bureau (NCRB), Crime in India 2021: Statistics (Government of India, 2022)

Morphing: Morphing includes altering or editing a photo or video of a woman to create fake sexual content with the intention of causing harm to the reputation and dignity of a woman.

Impersonation: Impersonation or fake profile is defined as creating a fake account of a woman in her name on social media with the intention to spread misinformation about her.

Phishing: Phishing is a financial exploitation that tricks a woman by sending fraudulent emails, texts, or messages to reveal sensitive information, such as bank details or passwords, with the intention of financial gain. With the rise of scams, scammers are most likely to target women.

Cyber Blackmailing: In this, the blackmailer blackmails a woman to leak private chats, photos or videos and demands money or sexual favours.

Digital Voyeurism: It is the act of secretly recording a woman engaging in private activities for sexual pleasure, using technology such as cameras, smartphones, drones and any other technology. This hampers the privacy of women.

Doxxing: Doxxing is a form of cybercrime in which a woman's private or personal information is shared on a social media platform without their consent.

Cyber Defamation: This is also known as Online Defamation, which means publishing false information against a woman in an online or social media platform with the intention to harm the reputation and dignity of a woman.

Cyber Grooming: Cyber grooming is a process of making a relationship with young women through the internet with the intention of gaining trust and later exploiting them sexually, mentally and financially.

Cyber Sextortion: It is a form of cybercrime in which a person threatens or blackmails a woman by internet device with a demand to share sexual favours, private photos or videos and a continuing supply of more content.

Cyber Pornography: Cyber pornography refers to publishing, transmitting, distributing or accessing pornography material through the internet.

Cyber Trafficking: Unlike sex trafficking, the victim does not come in direct contact with the abuser, but the victim is called for sexual favours through the internet, such as live-streaming, photos or videos performing sexual acts.

Cyber Mobbing: Cyber mobbing is a form of cyberbullying where a group of people, through technological devices, harass, insult or abuse a woman on social media platforms.

Identity theft: This crime refers to the misuse of someone's personal identity or information, such as bank details, passwords, fingerprints, or voice samples, with the intention to cause injury to someone.

STUDY OF CYBER CRIME AGAINST WOMEN WITH LEGAL PERSPECTIVE IN INDIA

Information Technology Act, 2000

Section 66A: Punishment for sending offensive messages through communication service, etc.[3] This section was added by the 2008 Amendment in the Information Technology Act,2000. This section talks about the offensive messages sent by any computer resource or communication device. Section covers:

1. Character of information can be:
    - Grossly offensive
    - Menacing
2. Information can be false with the purpose of causing:
    - Annoyance, Inconvenience, Danger, Obstruction, Insult, Injury, Criminal Intimidation, Enmity, Hatred and Ill Will
3. Sending electronic mails for the purpose of causing:
    - Annoyance, Inconvenience and Mislead

Punishment: Imprisonment for a term which may extend to three years and a fine.

Section 66C: Punishment for identity theft.[4] This section deals with any person who dishonestly or fraudulently uses another person's electronic signature, password or any other unique identification.

Punishment: Imprisonment for a term which may extend to three years and a fine not more than 1 lakh.

[3] Information Technology Act 2000, s 66A (inserted by the Information Technology (Amendment) Act 2008)
[4] Information Technology Act 2000, s 66C

Section 66D: Punishment for cheating by personation by using a computer resource.[5] Section 66C deals with identity theft, and Section 66D deals with cheating with identity theft. This involves cheating by personation with the use of a computer device or computer network.

Punishment: Imprisonment for a term which may extend to three years and a fine which may extend to 1 lakh.

Section 66E: Punishment for violation of privacy.[6] This section deals with the person who intends to capture, publish or transmit the image of the private area of any person without their consent, which leads to violating the privacy of that person.

Punishment: Imprisonment for a term which may extend to three years and a fine not more than 1lakh.

Section 67: Punishment for publishing or transmitting obscene material in electronic form.[7] This section deals with the person who transmits or publishes in electronic form any lascivious material, prurient material, or matter that will deprave and corrupt persons who are likely to read, see or hear it.

Punishment: For first conviction, imprisonment for a term which may extend to three years and a fine may extend to 5lakh. And for a second and subsequent conviction, imprisonment for a term which may extend to five years and a fine may extend to 10lakhs.

Section 67A: Punishment for publishing or transmitting material containing a sexually explicit act, etc., in electronic form.[8] This section deals with a person which transmit or publishes sexually explicit acts or conduct in electronic form shall be punishable with imprisonment for a term which may extend to five years and a fine may extend to 10lakhs. And for a second and subsequent conviction imprisonment for a term which may extend to seven years, a fine may extend to 10 lakhs.

[5] Information Technology Act 2000, s 66D
[6] Information Technology Act 2000, s 66E
[7] Information Technology Act 2000, s 67
[8] Information Technology Act 2000, 67A

BHARATIYA NYAYA SANHITA, 2023

Section 75: Sexual assault.[9] This section deals with a man committing any offence such as making physical contact with women, demanding/requesting for sexual favour, showing pornography against her will, shall be punishable with rigorous imprisonment for three years and fine or both or making sexually colours remarks shall be punishable with imprisonment for term not more than one year or fine or both, even through electronic means.

Section 76: Assault or use of criminal force on a woman with the intent to disrobe.[10] This section covers when any person uses force or assault against a woman or compels her to be naked, whether in a virtual platform, shall be punishable with imprisonment for a term not less than three years, which may extend to seven years and a fine.

Section 77: Voyeurism.[11] Any person who watches or captures the image of a woman engaging in any private activity when she expects not to be observed. This will expand to digital voyeurism, which includes watching, capturing or taking images/videos of women engaging in private activity through smartphones, cameras, or any other electronic device.

Punishment: For first conviction, imprisonment for a term not less than one year, which may extend to three years and a fine. And for a second or subsequent conviction, imprisonment for a term not less than three years, which may extend to seven years and a fine.

Section 78: Stalking.[12] If a man follows a woman**,** contacts or attempts to contact a woman to interact, even after several disinteractions and monitors her by the use of internet, email or other electronic communication shall be liable under this section.

Punishment: For first conviction, imprisonment for a term not less than one year, which may extend to a term of three years and a fine. For a second or subsequent conviction, imprisonment for a term not less than one year, which may extend to five years and a fine.

Section 79: Word, gesture or act intended to insult the modesty of a woman.[13] This section criminalises such acts which outrage the modesty of a woman by saying any word, making any

[9] Bharatiya Nyaya Sanhita 2023, s 75
[10] Bharatiya Nyaya Sanhita, s 76
[11] Bharatiya Nyaya Sanhita, s 77
[12] Bharatiya Nyaya Sanhita, s 78
[13] Bharatiya Nyaya Sanhita, s 79

sound, gesture or exhibiting any object, that such word or sound can be heard or such gesture or object seen by her, even though online platforms.

Punishment: Simple imprisonment for a term not less than one year, which may extend to three years and a fine.

THE PROTECTION OF CHILDREN FROM SEXUAL OFFENCES(POSCO) ACT, 2012

Section 3: Penetrative Sexual Assault.[14] This section covers crimes against the girl child to be sexually assaulted through penetration of the penis into the vagina, mouth, urethra or anus or insert any object/body part into the vagina, urethra or anus or manipulate her for penetration or apply mouth to a sexual organ or a child. Any person convicted under this section shall be punishable under section 4,[15] imprisonment for a term not less than 10 years, which may extend to imprisonment for life and a fine. Any person who is convicted of the offence on a child below sixteen years of age shall be punishable with imprisonment for a term not less than twenty years, which may extend to imprisonment for life, and a fine.

It is relevant to cybercrime if the child is exploited on an online platform, or if it can be digitally recorded or live-streamed.

Section 5: Aggrieved Penetrative Sexual Assault.[16] This section deals with penetrative sexual assault that is aggrieved when committed by a police officer, member of an armed or security force, a public servant, a member of a hospital, educational institution or religious institution or a gang using a deadly weapon, fire or heated substance, causing bodily harm and grievous hurt to the child below twelve years of age. Any person who commits aggrieved penetrative assault shall be punishable under section 6,[17] rigorous imprisonment for a term not less than twenty years, which may extend to imprisonment for life and fine or death. This offence is relevant to cybercrime if it can be recorded by electronic means or uploaded to any digital platform.

[14] Protection of Children from Sexual Offences Act 2012, s 3
[15] Protection of Children from Sexual Offences Act 2012, s 4
[16] Protection of Children from Sexual Offences Act 2012, s 5
[17] Protection of Children from Sexual Offences Act 2012, s 6

Section 7: Sexual Assault.[18] This section covers sexual assault of a girl child without penetration, such as physical contact with sexual intent. It is relevant to cybercrime if the person sends sexual messages, mails include cyber grooming or online harassment. Any person who commits sexual assault shall be punishable under section 8,[19] imprisonment for a term not less than three years, which may extend to five years and a fine.

Section 9: Aggrieved Sexual Assault.[20] This section deals with sexual assault that is aggrieved when committed by a police officer, a member of an armed or security force, a public servant, a member of a hospital, an educational institution, a religious institution or a gang using a deadly weapon, fire or heated substance causing bodily harm and grievous hurt to a child below twelve years of age. Any person who commits aggrieved penetrative assault shall be punishable under section 6,[21] rigorous imprisonment for a term not less than five years, which may extend to seven years and a fine. This offence is relevant to cybercrime if it can be recorded by electronic means or uploaded to any digital platform.

Section 11: Sexual Harassment.[22] Sexual harassment may include, any person making any sound, word or gesture or object which can be heard or seen by a child, showing pornography material to them, continuously or repeatedly follow, watch or contact a child either through electronic, digital or other means, threaten to use real or fake images or videos of child in sexual act in electronic and digital mode with sexual intent. Any person who is convicted under this offence shall be punishable under section 12,[23] imprisonment for a term which may extend to three years and a fine.

Section 13: Use Of a Child for Pornographic Purposes.[24] This section covers the use of children in media for sexual pleasure. This includes assaulting/threatening a child to expose them to pornography material, recording a child engaging in a sexual act, live streaming of such acts or obscene representation of a child. Any person who is convicted under this offence shall be punishable under section 14,[25] imprisonment for a term not less than five years and a fine for the first conviction, and imprisonment for a term not less than seven years and a fine.

[18] Protection of Children from Sexual Offences Act 2012, s 7
[19] Protection of Children from Sexual Offences Act 2012, s 8
[20] Protection of Children from Sexual Offences Act 2012, s 9
[21] Protection of Children from Sexual Offences Act 2012, s 10
[22] Protection of Children from Sexual Offences Act 2012, s 11
[23] Protection of Children from Sexual Offences Act 2012, s 12
[24] Protection of Children from Sexual Offences Act 2012, s 13
[25] Protection of Children from Sexual Offences Act 2012, s 14

THE IMMORAL TRAFFIC (PREVENTION) ACT, 1956

Section 5: Procuring, inducing or taking a person for the sake of prostitution.[26] This section applies to a woman or girl, without her consent, to procure or induce for prostitution on an online platform.

Punishment: Rigorous imprisonment for not less than three years and not more than seven years, and a fine of up to two thousand rupees. And if the offence is committed against the consent of the woman or girl, then the punishment shall be imprisonment for a term of seven years, which may extend to fourteen years.

Section 6: Detaining a person in premises where prostitution is carried on.[27] This section punishes a person who detains a woman or girl with/without their consent in a brothel or premises where women are compelled to be prostitutes.

Punishment: Imprisonment for not less than seven years, which may extend to Imprisonment for ten years or may be for life and a fine.

This section can be relevant to cybercrime in the form of cyber sextortion, online detention, online recruitment or cyber trafficking.

THE COPYRIGHT ACT, 1957

Section 63B: Knowing use of an infringing copy of a computer programme to be an offence.[28] This section protects a woman from data theft. If any person makes use of an infringing copy of a computer programme knowingly, they shall be punishable with imprisonment for a term not less than seven days but may extend to three years and a fine not less than fifty thousand rupees, which may extend to two lakhs.

STUDY OF CYBER CRIME AGAINST WOMEN THROUGH CASE LAWS

State of Tamil Nadu v. Suhas Katti (2004):[29] In this case, the accused Suhas Katti wanted to marry the victim, Ms Roselind, but she refused and married the love of her life. After one year, she got divorced from her husband. After the divorce, the accused approaches the victim again

[26] Immoral Traffic (Prevention) Act 1956, s 5
[27] Immoral Traffic (Prevention) Act 1956, s 6
[28] The Copyright Act 1957, s 63B
[29] State of Tamil Nadu v Suhas Katti [2004] CC No. 4680/2004 (Chief Metropolitan Magistrate, Egmore)

and asks to marry, but she rejects. Still, the accused did not stop and created a fake Yahoo account and a fake email ID (roosean@yahoo.com.in) in the name of the victim. The accused posted obscene and defamatory messages by impersonation in the five Yahoo groups. He also shared the phone number of the victim in the group, which led to a number of people calling and harassing her, and then the accused filed a complaint on 5th November 2004 in the cybercrime cell, Chennai. Later, it was found that the crime was operated from Mumbai.

The court found the accused guilty and convicted him under Section 67 of the IT Act, 2000[30] (punishment for publishing or transmitting obscene material in electronic form), Section 469, IPC[31] (section 336 BNS, 2023[32] – forgery for the purpose of harming reputation) and section 509, IPC[33] (section 79 BNS, 2023[34] – word, gesture or act intended to insult the modesty of a woman), he was sentenced to rigorous imprisonment for a term of two years and a fine under section 469 IPC(section 336 BNS, 2023), imprisonment for a term of one year and a fine under section 509IPC (section 79 BNS, 2023). And rigorous imprisonment for a term of two years and a fine under section 67 of the IT Act, 2000.

Kalandi Charan Lenka v. State of Odisha (2017):[35] In this case, the victim is the female student studying at Pattamundai Women's College. She received an obscene message on her phone, and a similar message was also sent to her father. During the year 2015-16, the victim's father received a letter in vulgar language, causing defamation with an impersonated sexual remark. Then, a pamphlet defaming the victim's character was found posted on the wall of the hostel where the victim resided. This led her to change the place of study. The harassment continues, and then the accused created a fake Facebook account in the victim's name, where he shares morphed nude photos of the victim. Then the victim filed a complaint against the accused, Kalandi Charan Lenka.

The accused was arrested by the police. He was convicted under section 66C[36] (identity theft), section 66D[37] (cheating by personation usind a computer resource) and section 67[38] (publishing

[30] Information Technology Act 2000, s 67
[31] Indian Penal Code 1860, s 469
[32] Bharatiya Nyaya Sanhita 2023, s 336
[33] Indian Penal Code 1860, s 509
[34] Bharatiya Nyaya Sanhita, s 79
[35] Kalandi Charan Lenka v State of Odisha [2017] SCC OnLine Ori 36 (Orissa HC)
[36] Information Technology Act 2000, s 66C
[37] Information Technology Act 2000, s 66D
[38] Information Technology Act 2000, s 67

or transmitting obscene material in electronic form) of IT Act, 2000 and section 354D IPC[39] (section 78 BNS,2023[40] – stalking), section 469 IPC (section 336 BNS, 2023– forgery for the purpose of harming reputation) and section 509 IPC(section 79 BNS, 2023 – word, gesture or act intended to insult the modesty of a women). The accused applied for bail, but the Orissa High Court rejected it as the offence is serious and damaged the reputation and dignity of the victim.

Shreya Singhal v. Union of India (2015):[41] In 2012, two girls, Shaheen Dhada and Rinu Srinivasan from Maharashtra, were arrested under section 66A of the IT Act, 2000 for posting their remark on Facebook on the Shivsena's death. Under Article 32 of the Constitution of India, a petition was filed to the Supreme Court by a petitioner, Shreya Singhal, who is a law student, challenging the constitutionality of Section 66A, IT Act, 2000. The issue raised before the court was whether the section 66A, IT Act,2000 violate the Article 19(1)(a)[42] of the Constitution of India.

The Supreme Court held that section 66A, IT Act, 2000, unconstitutional as it violates Article 19(1)(a) and it is not safe under Article 19(1)(a). It was a huge milestone in Indian cyber law and constitutional law.

CAUSES OF CYBER CRIME AGAINST WOMEN IN INDIA

There are three main causes for cybercrime against women in India. The first one is a societal and cultural factor, the second one is the technology gap and security measures, and the third one is legal and enforcement challenges.

One of the reasons under societal and cultural factors is misogyny, hating and disliking of women, women are objectified and targeted online easily because of their gender. The Indian society still follows the old patriarchal system, where men are seen as dominant and women are submissive. That's why the man treats women as objects instead of treating them equally. Along with the physical world, social media platforms are also not a safe place for women; they are harassed just because they speak up and share their opinions.[43] The other reason can

[39] Indian Penal Code 1860, s 354D
[40] Bharatiya Nyaya Sanhita 2023, s 78
[41] Shreya Singhal v Union of India [2015] 5 SCC 1 (Supreme Court of India)
[42] Constitution of India 1950, art 19(1)(a)
[43] Shruti Bedi, 'Cyber Crime against Women in India: Causes and Consequences' (Legal Service India, 2022)

be gender bias and victim blaming, when the woman gets harassed, instead of blaming the offender, society blames the victim and questions her behaviour, clothes, and online activity.

The second cause is the technology gap and security measures; in this, both the individual and the online platform fail to maintain cybersecurity. Lack of cybersecurity can increase crime against the vulnerable group of women. Many women use weak passwords, which give criminals a chance to hack the password easily and have easy access to their private photos, personal information and online activity, which makes blackmailing and stalking easy for them.[44] Nowadays, the number of women there is on the rise, and many of them don't know how to use privacy settings. The cyber criminals take advantage of the lack of awareness among women and trick them easily into fraud, identity theft and many other cybercrimes.[45]

As there are merits of advancement in technology, there are demerits too. The advancement in technology gives tools and methods to cyber criminals to commit cybercrime. These advanced methods provide a way to exploit and harass women.[46]

IMPACT OF CYBER CRIME AGAINST WOMEN ON WOMEN IN INDIA

Psychological and Emotional Impact: Cybercrime, such as cyberbullying, cyber stalking, online harassment, financial fraud and many other cybercrimes can cause psychological and emotional impact on the victim. They suffer from social humiliation, social stigma, trauma, stress, depression, low self-esteem, constant fear of being targeted, a sense of insecurity and loss of confidence. This can also push women to suicidal thoughts or self-harm.

Social Impact: Indian society often sees women as an inferior section of society, and women even face victim blaming, where their character, behaviour and clothing are questioned, instead of blaming the offender. This can impact women in social isolation, societal fear, restriction from family members, public shame, harm to reputation, and digital crime against women, which may impact family honour and community status.[47]

Economic Impact: Due to a lack of awareness among some women, they are tricked easily by such cybercrime. They can be targeted for financial scams such as online fraud, identity theft,

[44] 'Cybercrime against Women in India' (Law Times Journal, 10 March 2022)
[45] National Crime Records Bureau (NCRB), Crime in India 2021: Statistic (Government of India, 2022)
[46] Shruti Bedi (n 43)
[47] Law Times Journal (n 44)

blackmail for money, and sending fake emails can lead to loss of money. Injury to reputation or public shame leads to loss of job or leaving one's job.[48]

Privacy and Reputation Hampers: Crimes such as cyber stalking, cyber hacking, voyeurism, morphing, impersonation, doxxing, mobbing, and identity theft may violate the privacy and reputation of the women. The violation of privacy may include continuously and repeatedly tracking the online activity of women, which makes her feel constantly watched by someone. Leaking or posting of personal or morphed, deepfake photographs or videographs can harm the reputation of women. The use of women's personal details for financial scams leads to the violation of digital privacy and monetary loss.[49]

Long Term Consequences: The long-term consequences of cybercrime against women can permanent psychological impact such panic attacks, depression, anxiety, permanent privacy and reputation harm like if private photo of a women or secretly recording a women engaging in private conduct is posted on any social media platform and even it is erased, still that can leave a long-term impact on women's privacy and reputation. Financial scam leads to financial burden for a long time. This can also impact women's minds; she got afraid to share or post her opinions or photos on social media platforms, and she reduced her use of social media. Sometimes she started thinking or started to change herself because of victim-blaming.

CONCLUSION

The cybercrime against women is a growing global issue. These crime exposes women to harassment, assault, and exploitation. The various forms of cybercrime impact women from social humiliation to social isolation, from depression to family and community status pressure and from violation of privacy to financial impact, which affects the overall mental health of a woman broadly. Many legal frameworks and judicial interpretations, such as the Information Technology Act, Bharatiya Nyaya Sanhita, POSCO Act, Immoral Trafficking Act, explain the various forms of cybercrime committed against women and their punishments.

[48] NCRB (n 45)
[49] Shruti Bedi (n 40)