IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Crime Against Women in India

Ms Nikke

Assistant Professor of Law

Department of Law,

Gurugram University, Gurugram

Abstract:

Indian civilization boasts one of the world's oldest heritages.
The status of women was very respectable in ancient Indian culture.

'यत्र नार्यस्तु पूज्यन्ते रमन्ते तत्र देवता'[1]

This means that where women are worshipped, respected, the gods reside there. Where women are not worshipped, all (even the best) activities (karmas) become fruitless. However, there has been a noticeable uptick in crimes against women in India, dating back to the era of external invasions. Whether in ancient or modern times, crimes against women have persisted, albeit now taking on new forms and platforms. While such crimes were once confined to the physical realm, they now manifest in the cyber world, encompassing activities like eve teasing, bullying, abuse, harassment, and blackmailing. In the age of information technology, cyber crimes against Indian women proliferate in cyberspace, including harassment through email, cyber-stalking, defamation, morphing, spoofing, hacking, pornography, sex trafficking, and eve teasing. However, the current laws in India are insufficient to effectively address cyber crimes. There is an urgent need to bolster and rigorously enforce these laws to combat cyber crimes more effectively. At the same time, awareness drive by Government and NGOs, Universities to educate women about cybercrime are also required.

Key Words: Cyber Crimes, Cyber crime against women, Cyber stalking, Cyber defamation, Cyber trolling, Cyber pornography, Cyber bullying, Cyber grooming, Cyber phishing

Introduction

In 2022, India experienced a 24% surge in cybercrimes compared to the previous year, as indicated by the latest data from the National Crime Records Bureau. Additionally, various other crime categories, such as economic offenses (11%), crimes against senior citizens (9%), and crimes against women (4%), also witnessed an uptick. According to the 'Crime in India' report, there were 65,893 cybercrime cases registered, reflecting a 24.4% increase from 2021. The majority of these cases, 64.8%, were related to fraud, followed by extortion at 5.5% and sexual exploitation at 5.2%.[2]

Cyber Crime

In Indian legislation, the term 'cyber crime' remains undefined. However, 'cyber' typically pertains to computers, the internet, or technology, suggesting that cyber crimes involve offenses perpetrated in the virtual realm utilizing the internet.

Cyber Crime against women

Cyber offenders leverage technology to access personal data and victimize women. Examples of cyber crimes against women encompass sending inappropriate emails or messages via platforms like WhatsApp, cyberstalking, creating explicit content, forging emails, altering images, and more. Perpetrators often use fake social media profiles to intimidate and extort their victims. Their motivations range from financial gain and revenge to humiliating the victim, extortion, sexual abuse, defamation, and other malicious intents. For instance, it's feasible to digitally manipulate a woman's image into explicit content. Cyberstalking entails harassing someone online, causing psychological distress and suffering to the victim by gathering information and issuing threats through various digital means.

History of Cyber crime in India

In 2001, Ritu Kohli became the first reported victim of cyber stalking in India. She filed a complaint with the police against an individual impersonating her online, sharing her personal information, and using vulgar language. Her contact details were leaked, resulting in unwanted calls at odd hours. The police traced the IP address, leading to the arrest of Manish Kathuria under Section 509 of the Indian Penal Code for outraging Ritu Kohli's modesty. However, this section only addresses physical acts, not cyber offenses. This case highlighted the lack of specific laws in India regarding cyber stalking and women's protection. Consequently, Section 66A was added to the Information Technology Act, 2008, prescribing imprisonment and fines for sending offensive messages through communication services.

Indian Laws regulating cyber crimes against women

Indian laws encompass numerous provisions regulating cyber crimes, often with considerable redundancy. Specifically, three legislations focus on addressing cyber crimes targeting women.

Indian Penal Code

Initially, the IPC lacked specific provisions dealing with cybercrimes targeting women. However, in 2013, a shocking gang-rape incident occurred in New Delhi, triggering widespread public outcry. In response to this outcry, the Criminal Amendment Act of 2013 was enacted, amending the Indian Penal Code and incorporating sections 354A to 354D.

Section 354A pertains to sexual harassment and its associated penalties. It sanctions a man for engaging in the following behaviors:

Soliciting a sexual favor from a woman
Displaying pornography without the woman's consent
Uttering sexually suggestive remarks

Section 354D deals with the crime of stalking, which encompasses cyberstalking as well. This provision applies to individuals who monitor women's activities on the internet, email, or other electronic communication platforms. Upon the first conviction, such individuals may be subject to three years of imprisonment, a fine, or both. Repeat convictions could lead to imprisonment for up to five years.

2. The Information Technology Act, 2000 (IT Act)

As cybercrimes escalated, the IT Act of 2000 underwent revisions in 2006 and subsequently in 2008. The Information Technology (Amendment) Act of 2008 brought forth several sections aimed at governing cybercrimes.

Section 66C of the legislation renders identity theft a punishable offense. Violating this section by engaging in identity theft or utilizing someone else's password or electronic signature can result in imprisonment for up to three years and a fine of up to one lakh rupees.

Section 66E addresses breaches of privacy. Disseminating or transmitting private images without consent is subject to a penalty of up to three years' imprisonment or a fine of two lakh rupees or more.

Under Section 67A, the publication, transmission, or facilitation of transmission of obscene content is prohibited. Those convicted under this provision may face imprisonment for three years and a fine for the initial conviction, with subsequent convictions potentially resulting in imprisonment for up to five years.

Section 72 establishes consequences for breaches of confidentiality and privacy. Individuals found guilty of such violations may be sentenced to up to two years' imprisonment, fined one lakh rupees, or both.

3. The Indecent Representation of Women (Prohibition) Act, 1986

The Indecent Representation of Women (Prohibition) Act, 1986, oversees and forbids the inappropriate portrayal of women in advertisements, publications, and other mediums. Section 2 defines such depiction as any representation that undermines public morality. The Rajya Sabha introduced the Indecent Representation of Women (Prohibition) Bill in 2012, with the objective of extending its coverage to audio-visual media and electronic content, including material distributed on the internet and the depiction of women online. However, the bill was subsequently retracted.

Existing Gaps In The Legislation

The existing gaps in the legislation regarding cyber crimes against women are as follows:

1. The IT Act does not include gender-specific crimes. The use of the term "whoever" in the Act indicates its non-gender-specific nature. There are no delineated crimes or penalties in the Act specific to any gender. Individuals convicted of cyber crimes would face identical penalties regardless of their gender. This implies that the amendments to the Act were not specifically aimed at addressing the increase in cyber crimes against women. In contrast, the Indian Penal Code (IPC) introduced gender-specific provisions. However, such provisions are absent in the IT Act, which instead features more general provisions. Incorporating gender-specific provisions is crucial as it acknowledges violence against women as a form of gender-based discrimination and caters to the distinct needs of female survivors.

2. Another flaw exists in the narrow interpretation of privacy violation within the IT Act. It solely covers the transmission, publication, or capture of an "image of a private area of the body," explicitly mentioning the buttocks and female breasts. This limited interpretation confines a woman's privacy solely to her physical form, implying that her privacy is limited to her body. However, privacy violation can occur without the explicit capturing of images. The Act's provision on privacy is limited in scope, failing to acknowledge that women are more than just their physical bodies. We shouldn't narrowly define privacy within the Act, as it encompasses various aspects beyond physical appearance.

3. The notion of consent holds significant importance in such instances. Demonstrating that the victim did not consent to the publication of such images can be daunting. Even married women have fallen prey to cyber crimes, where, for instance, a separated husband may upload intimate pictures of his wife. In such situations, proving a lack of consent becomes challenging. Fewer cases are filed under section 66E of the Act, leading to a negligible conviction rate under the Act.

4. The Indecent Representation of Women Act, 1986, is underutilized in legal practice. Its primary focus is not on delivering justice to victims but rather on granting authority to the state to act against indecent representation. The Act empowers the state to take punitive measures as necessary. Despite its title implying a focus on women, the Act predominantly revolves around preserving public morality. Notably, any exposure of a woman's body is considered indecent. There are various ways women can be indecently represented, beyond just their physical form. However, this Act fails to address the online harassment women endure. Furthermore, the number of cases filed under this Act has declined over time, rendering it less relevant due to its significant loopholes.

5. Cyber crime victims frequently lodge complaints under the IT Act. Although it might facilitate easier arrests by the police, they often lack familiarity with the latest technologies. Consequently, they encounter challenges in filing chargesheets and tracing the genuine source of these crimes. The court frequently acquits individuals arrested under the Act due to insufficient evidence.

6. Insufficient awareness of cyber crime laws constitutes a significant gap in addressing cyber crimes against women. Consequently, the number of reported cases under these Acts remains low. If law enforcement agencies confine themselves to merely recording and probing cases, this problem will persist. Hence, it is imperative to undertake initiatives to educate and sensitize people about the laws and their entitlements. Despite being in 2023, many women are still uninformed about cyber laws, including the remedies accessible to them. Furthermore, victims often lack knowledge about the correct procedures for lodging complaints. Some feel ashamed about reporting incidents, thus prolonging the ongoing harassment.

7. Existing legislation primarily concentrates on safeguarding against physical harm, neglecting to adequately address the mental distress caused by cyber crimes. Despite prioritizing the physical safety of women, these laws fail to encompass the mental harm endured by victims throughout the ordeal.

Government Initiative to curb Cyber crime and promote awareness about cyber crimes:

"Policing" and "Public Order" fall under the jurisdiction of the states according to the Seventh Schedule of the Indian Constitution. Therefore, states and union territories (UTs) bear primary responsibility for preventing, detecting, investigating, and prosecuting crimes, including cybercrimes, through their Law Enforcement Agencies (LEAs). These agencies take legal action against offenders as per the provisions of the law. The Central Government supports state initiatives through advisories and financial assistance under various schemes aimed at enhancing their capacity.

According to the Ministry of Home Affairs (MHA), to enhance the mechanism for addressing cybercrimes comprehensively and coordinately, financial assistance has been provided to all states and UTs under the Cyber Crime Prevention against Women & Children (CCPWC) scheme. This support aims to help them establish cyber

forensic-cum-training laboratories, provide training, and recruit junior cyber consultants. Cyber forensic-cum-training laboratories have been set up in 28 states. The Scheme for Cyber Crime Prevention against Women and Children (CCWC) has been formulated by the Ministry of Home Affairs to have an effective mechanism to handle cybercrimes against women and children in the country.

Components of the CCPWC Scheme

- Online Cybercrime reporting Unit
- Forensic Unit
- Capacity Building Unit
- Research & development Unit
- Awareness Creation Unit

The Central Government also focuses on raising awareness about cybercrimes, issuing alerts/advisories, enhancing capacity through training for law enforcement personnel, prosecutors, judicial officers, and improving cyber forensic facilities.

The Government has established the Indian Cyber Crime Coordination Centre (I4C) to create a framework and ecosystem for LEAs to address cybercrimes comprehensively and coordinately. "Joint Cyber Coordination Teams" have been formed for seven regions in Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under the I4C to tackle jurisdictional complexities based on cybercrime hotspots/areas, involving all states/UTs to provide a robust coordination framework to the LEAs.

The Government has launched the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) to enable the public to report incidents related to all types of cybercrimes, with a particular focus on those against women and children. This portal allows to register women and children related crime anonymously[3]. Only Child Pornography (CP) - Child Sexual Abuse Material (CSAM), Rape Gang Rape (RGR) - Sexually Abusive Content and Sexually Explicit Content related complaints can be reported through this option.

The National Cyber Crime Reporting Portal can be used to report complaints related to:

- Online child pornography
- Child sexual abuse material
- Sexually explicit content such as rape/gang rape content
- Mobile crimes
- Online and social media crimes
- Online financial frauds
- Ransomware
- Hacking
- Cryptocurrency crimes
- Online cyber trafficking

A toll-free number 1930 has been activated to assist in lodging online cyber complaints. Additionally, the Citizen Financial Cyber Fraud Reporting and Management System module has been introduced for immediate reporting of financial frauds and to prevent fund siphoning by fraudsters.

The National Commission for Women (NCW) has several initiatives to promote awareness about cyber crime:

[4]Digital Shakti

- Launched in 2018, this program helps women learn about cyber safety tips, reporting, data privacy, and technology usage. As of November 2022, more than 300,000 women across India have participated in the program. It's latest edition Digital Shakti 4.0 is a pan-India project that aims to help women and girls become digitally skilled and aware. The campaign was launched in November 2022 by the National Commission for Women (NCW) in collaboration with Meta and Cyber Peace Foundation.

The campaign's goals include:

- Helping women and girls navigate the digital landscape safely and confidently
- Creating safe spaces for women and girls online
- Making women digitally skilled and aware to stand up against any illegal/inappropriate activity online
- Helping women raise awareness levels on the digital front

Digital Literacy and Online Safety Programme

This program aims to train 60,000 women in universities across India on how to use the internet, social media, and email safely. The program also helps women differentiate between credible and questionable information online.

During 2020-21, the Commission in collaboration with Universities/Colleges, has undertaken 5 Research Studies on **"Cyber Security and threats in Cyber Space faced by Women".** The Commission has also been focusing on spreading awareness on cyber crimes by making it a part of various Legal Awareness Programs.[6]

The Commission also organized a Webinar on **Misogyny Online and Social Responsibility of Social Media** on 23rd June 2021, with the focus on internet etiquette, Gender equity policies and community guidelines of Social media platforms .[7]

In case of any complaint received by the Commission, pertaining to Cyber crime against women, the matter is immediately taken up with the concerned authorities including police Cyber cells of MHA for taking appropriate action in the case. The Commission has launched an awareness campaign by developing a creative/video spot on cyber crime security and is disseminating information through social media platforms.

Conclusion:

The cybercrime data in India indicates that the current methods for preventing cybercrimes are inadequate. This deficiency could be attributed to various factors, each contributing to how women experience such crimes and how law enforcement investigates them. Apart from broader systemic issues related to crimes against women, specific factors affecting victimization and investigation concerning cybercrimes include:

- Scarce understanding of cyber threats and necessary precautions.
- Limited familiarity with legal frameworks and policy measures for protection and resolution.
- Insufficient cooperation and assistance from internet service providers.
- Lack of proper infrastructure and expertise for conducting investigations.

Reference:

1. Chapter 3, Manu Samriti
2. "Crime in India" report of NCRB
3 USER MANUAL FOR NATIONAL CYBERCRIME REPORTING PORTAL
4. https://cybercrime.gov.in/
6. NCW website http://ncw.nic.in/
7. NCW website http://ncw.nic.in/