

Cyber Crime Against Women and Children in India

Dr. Anoop Kailasia*

*Assistant Professor (Law) Govt. Law College, Gwalior (M.P.) INDIA

Abstract : The internet is one of the most effective communication tools available, and Indians use the most internet data worldwide. As industrialization and technical breakthroughs increased, the realm of cyberspace saw an exponential growth in the potential and characteristics of the internet. It may be used for both constructive and negative impact. The distance significantly decreased, and we could now easily access any far-flung region of the globe. But emerging technology has also become a vehicle for cybercrime, or violence in cyberspace. Due to their ambiguity, cybercrimes are very difficult to trace back, which is why criminals frequently choose to commit them. Cyberspace violence blurs the boundaries of jurisdiction, and victims become more numerous as a result of ignorance and unfamiliarity. Women, children, and other vulnerable populations are the targets of the bulk of cybercrimes. Common instances include financial exploitation, child grooming, blackmail, and pornography. The Information Technology Act of 2000 (amended 2008) regulates such offenses. The current condition of cybercrimes against Madhya Pradesh's women and children will be discussed in this article. The findings presented in this article are derived from a research study focused on this topic. Overall, there is a need to explore the methods of executing cybercrimes and to propose specific measures to prevent and manage cybercrime targeting women and children in cyberspace.

Introduction - In India, cybercrimes against women and children are becoming a bigger problem. These crimes include child grooming, cyberstalking, cyberpornography, online harassment, cyberblackmail, and child pornography, which use digital platforms to reinforce offline harms. Due to societal factors and the increasing prevalence of the internet, women and children are particularly vulnerable and frequently targeted by digital abuse, including revenge pornography and deepfakes. There are calls for stronger legal frameworks and specialized investigative bodies, like the online cybercrime reporting portal, because, despite the fact that the Indian Penal Code, with sections like 354A, and the Information Technology Act, 2000, offer some legal recourse, it is difficult to address the complexity of these crimes.

Concept Of Cyber crime : One must first understand crime, which is connected to computers and the internet, in order to understand cybercrime. There is no difference between the idea of cybercrime and the idea of conventional offense. Whether by action or inaction, both entail actions that are against the law and are compensated for by the government. Cybercrime is distinct in that the victim and the offender may never come into direct contact. Bloodless and non-violent, cybercrime is committed through highly sophisticated means. The emergence of e-crime has made it difficult for the legal system to pinpoint instances of cloning being used in cybercrime.

India's Cyber Legislation For Women: In India, cybercrimes against women are addressed through a combination of provisions under the new Bharatiya Nyaya Sanhita (BNS, 2023), the Information Technology (IT) Act, 2000, and the Protection of Children from Sexual Offences (POCSO) Act, 2012. These laws cover a range of offenses, from cyberstalking and obscenity to identity theft and violation of privacy.

legal provisions for women's cyber safety in Bharatiya Nyaya Sanhita (BNS, 2023)

Section 78 (Stalking): Criminalizes following or repeatedly contacting a woman, electronically or otherwise, despite her clear disinterest.

Section 79 (Outraging the Modesty of a Woman): Addresses online actions like sharing offensive content or making derogatory remarks intended to insult a woman's dignity.

Section 77 (Voyeurism): Punishes capturing or distributing images of a woman engaged in a private act without her consent. Sharing images even with initial consent but not for dissemination is also an offense.

Section 351(4) (Criminal Intimidation): Covers threats made through anonymous communication on electronic platforms.

Information Technology (IT) Act, 2000

Section 66C (Identity Theft): Punishes the fraudulent use of a person's digital identity, including passwords or

electronic signatures, which is common in cases of creating fake profiles.

Section 66D (Cheating by Personation): Addresses using a computer resource to impersonate another person for harassment.

Section 66E (Violation of Privacy): Punishes capturing, publishing, or transmitting images of a person's private parts without their consent, often used for cases of "revenge porn".

Section 67 (Publishing Obscene Content): Prohibits publishing or transmitting obscene material in electronic form.

Section 67A (Publishing Sexually Explicit Content): Prescribes stricter punishment for disseminating sexually explicit material.

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: Hold social media platforms accountable for user safety and require them to remove violating content within specified timelines.

Government initiatives and support systems:

National Cyber Crime Reporting Portal (cybercrime.gov.in): A central government portal where anyone can report cybercrimes, with a special focus on crimes against women and children. It also allows for anonymous reporting in cases related to child sexual abuse material (CSAM) and explicit rape or gang rape content.

Cybercrime Prevention against Women and Children (CCPWC): A project by the Ministry of Home Affairs to create awareness, provide training to law enforcement, and improve cyber forensic facilities.

Digital Shakti Program: An initiative by the National Commission for Women (NCW) that aims to provide women with digital awareness and cyber safety tips.

Collect evidence: Take screenshots, save URLs, and preserve chat logs or emails related to the harassment.

File a complaint: Report the incident on the National Cyber Crime Reporting Portal or at the nearest police station or cybercrime cell.

Seek support: Contact legal experts, NGOs, or the NCW for assistance and guidance.

Cybercrime against children's : The increasing digitalization of daily life has led to a concerning rise in cybercrime against children in India. With more children accessing the internet for education, entertainment, and social connections, they are becoming increasingly exposed to online risks. This has been particularly exacerbated since the COVID-19 pandemic, where a shift to online schooling resulted in more screen time and digital isolation for children.

Scale of the problem

Rising statistics: According to data from the National Crime Records Bureau (NCRB), cases of cybercrime against children have been steadily increasing. A significant surge of 32% was reported between 2021 and 2022, with a total of 1,823 cases recorded in 2022.

Growing vulnerability: Children are vulnerable targets for

online predators due to their inherent trust, naiveté, and curiosity. Many lack the digital literacy to identify and assess online threats, making them susceptible to exploitation.

Diverse platforms: The risks appear across various platforms, including social media, chat rooms, online games, and encrypted messaging apps, which offer anonymity to malicious actors.

Common forms of cybercrime against children

Child Sexual Abuse Material (CSAM): The creation, publishing, and transmission of child sexual abuse material in electronic form is a severe and prevalent crime. Cases of this offense have shown a worrying increase, with 1,171 cases reported in 2022 alone.

Cyber grooming: Perpetrators befriend children online, often by using false identities and preying on their need for attention, with the intent of sexual exploitation.

Cyberbullying: The use of digital platforms to harass, threaten, and manipulate minors is widespread and can have severe psychological impacts, including anxiety and depression.

Sextortion and sexting: Criminals manipulate or pressure children into sharing explicit images, which are then used for blackmail or extortion.

Exposure to harmful content: This includes exposure to violent, pornographic, and inappropriate material that can cause severe emotional and mental harm.

Identity theft and fraud: Malicious actors can hack accounts to steal personal information for fraudulent purposes or impersonate the child.

Legal framework: India addresses cybercrime against children through a multi-pronged legal approach, drawing from several key acts:

Information Technology (IT) Act, 2000: This act includes provisions like Section 67B, which specifically penalizes the publication, transmission, or viewing of child sexual abuse material online.

Protection of Children from Sexual Offences (POCSO) Act, 2012: The POCSO Act provides for mandatory reporting of offenses and child-friendly procedures for recording evidence. It also criminalizes various forms of online sexual harassment, enticement, and pornography involving children.

Digital Personal Data Protection Act (DPDPA), 2023: This legislation aims to regulate how companies handle children's data, requiring verifiable parental consent for those under 18.

Government and public initiatives: The government has launched several initiatives to combat cybercrime and protect children online:

Indian Cyber Crime Coordination Centre (I4C): Established by the Ministry of Home Affairs, this center coordinates efforts among law enforcement agencies to deal with cybercrime.

National Cyber Crime Reporting Portal (www.cybercrime.gov.in): This portal allows the public to

report cybercrime incidents, with a specific focus on crimes against women and children.

POCSO e-Box: The National Commission for Protection of Child Rights (NCPDR) has set up an online platform for children or guardians to report sexual abuse cases.

Awareness campaigns: The government and NGOs regularly conduct awareness campaigns for parents, teachers, and students on online safety.

Ongoing challenges:

Jurisdictional issues: The global nature of the internet, with varied legal standards across countries, poses significant challenges in tracking and prosecuting offenders.

Lack of uniform legislation: Despite recent reforms, some legal gaps remain, including the lack of explicit legal provisions for certain crimes like online grooming and cyberbullying.

Underreporting: The stigma associated with sexual crimes and a lack of awareness among parents and children about reporting mechanisms often lead to underreporting.

Latest cybercrime statistics against women and children in India (2025): The latest available data on cybercrime in India indicates an increasing trend in cases reported against women and children. Here's a summary of the situation based on recent reports:

Overall rise in cybercrime: A total of 6,593,682 cybercrime incidents were reported to the National Cybercrime Reporting Portal (NCRP) from 2021 to June 2025.

There's been a significant surge in cybercrime cases in India, with reported losses crossing ₹ 22,845 crore in 2024, a 206% rise from 2023.

In 2024 alone, 36.37 lakh incidents of financial fraud were reported through the NCRP and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS).

Cybercrime against women: Nearly 20 lakh cybercrime complaints were recorded in 2024, and 1 in every 5 cases involved online abuse against women.

However, many women hesitate to report these crimes due to shame, dismissal, and a lack of understanding within the system regarding gendered trauma, according to an Instagram post by Her Circle.

According to MediaNama, funding for a women-focused cybercrime scheme dropped by 89% amidst the rising online abuse.

Cybercrime against children: The National Crime Records Bureau's (NCRB) 2022 report, the latest available, showed a 32% increase in cybercrimes against children, highlighting challenges in addressing online exploitation and child sexual abuse material (CSAM). Between 2018 and

2022, there has been a steady increase in cybercrime cases against children in India.

Conclusion: first and most important recommendation is that women should be courageous enough to confront the issue and warn their loved ones about such acts. The state and the federal government ought to enact new laws to combat this cybercrime. To sum up, cybercrime directed at women is a developing issue in India that has major ramifications for women's online safety and wellbeing. Prioritizing women's safety and wellbeing online is crucial, as is working to build a more just and inclusive society where women can enjoy their rights without worrying about violence or harassment.

Social media has become a lucrative target for criminals. Common crimes perpetrated online include stalking, honey trapping, and the release of personal information. The longer moms and kids spend online, without fully understanding the dangers of the internet, the more exposed they are. According to the survey, cybercriminals and female and child internet users in India are still vying for control of the internet's future. People are still afraid about the cyber apocalypse. Due to several shortcomings, the Indian Information Technology Act of 2000 is not being implemented efficiently, which leads to a rise in cybercrimes against women and children.

References:-

1. "Cyber Crimes against Women in India," by Dr. Ritu Sharma, published in 2019
2. "Women and Cybercrime in India: Challenges and Solutions," edited by Dr. Debarati
3. Halder and Dr. K. Jaishankar, published in 2017
4. C. Burgess-Proctor, "Understanding the Malevolent Use of Technology by Intimate
5. Partner Abusers," Violence Against Women, vol. 21, no. 8, pp. 995-1016, 2015.
6. Haldar, D., & Jaishankar, K. (2011), Victimization of Women in Cyber Space Cyber Crime and Victimization of Women :Law,Rights and regulations, IGI Global.
7. Vanita P.K. (2012), Cyber Crime against women- perception and opinion of cyber cell officials and counselors, Retrieved from
8. <https://oaji.net/articles/2021/1201-1610009923.pdf>
9. Dhirender Kumar (July 2018), Ministry of women and children, Retrieved from <https://pib.gov.in/PressReleasePage.aspx?PRID=1540340>
10. Shashya Mishra (Dec. 2018), Dimension of cybercrime against women in India, Retrieved from <https://www.ijrar.org/papers/IJRAR1944342.pdf>
11. Dharmraj, S. (2018), The current state of Cyber Security in India.
