Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

A Critical Analysis of the Efficacy of the Legal Framework in Addressing Cybercrimes Against Women and Children in India

[1]Prachi Diwan, [2]Akshat Tiwari, [3]Dr. Tarun Dhar Diwan
[1]Research Scholar, Department of Law, [2]Research Scholar
[1,2]Kalinga University, Raipur, Chhattisgarh, India
[3]Assistant Professor & Controller of Examinations, Atal Bihari Vajpayee University, Bilaspur, Chhattisgarh, India
[1]prachidiwan5@gmail.com

ABSTRACT

This study examined how well the primary legislative instruments governing cybercrimes against vulnerable populations in India include the Information Technology Act of 2000 and the Protection of Children from Sexual Offences (POCSO) Act of 2012. Together, these laws aim to regulate digital conduct and safeguard minors and women from online exploitation. Using a mixed-methods approach, the research includes data from the National Crime Records Bureau (NCRB) from 2017 to 2021, legal analysis, and selected case studies to provide a clear overview. The findings show a significant 63.5% rise in reported cybercrime cases during this time. Women made up 20.27% of the victims, while children accounted for 1.35%, demonstrating the increased risk these groups face online. The study points out several challenges, such as weak enforcement, low digital literacy, slow procedures, and the social stigma that stops victims from coming forward. To fill these gaps, the paper suggests specific actions: updating legislation, improving training for law enforcement, and launching public awareness campaigns about digital safety. These steps are vital for boosting India's cybersecurity and ensuring better protection for women and children in a increasingly digital landscape.

Keywords: Cybercrime, Women, Children, IT Act, POCSO Act, Digital Literacy, Legal Framework, India

1. INTRODUCTION

India’s digital transformation, with over 800 million internet users projected by 2025 (Ministry of Electronics and Information Technology, 2023), has revolutionized socio-economic interactions but also escalated cybercrimes targeting women and children. Offenses such as cyberstalking, online grooming, morphing, revenge pornography, and child sexual abuse material (CSAM), defined as visual depictions of minors in sexual contexts (Thomas, 2022), cause profound psychological, social, and reputational harm. Such crimes have serious effects beyond legal issues. Data from the National Crime Records Bureau (NCRB) shows a significant 63.5% increase in reported cybercrime cases, rising from 28,248 in 2018 to 44,546 in 2019. Women made up about 20.27% of the victims, while children accounted for 1.35%. This highlights the urgent need for targeted legal and institutional protections.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

India has put in place several legal mechanisms to handle cybercrime, especially those aimed at women and children. The three main legal frameworks include:

- The IT Act, 2000 (amended 2008), governs offenses such as digital identity theft, online stalking, and pornographic content distribution.
- The Protection of Children from Sexual Offences (POCSO) Act, 2012, which provides safeguards against online and offline sexual exploitation of minors.
- Relevant sections of the Indian Penal Code (IPC), such as Section 354D (stalking), Section 509 (insulting modesty), and Section 507 (criminal intimidation), address harassment-related offenses.

Despite these frameworks, enforcement is often inconsistent. Contributing factors include low digital literacy, limited access to cyber forensic tools, underreporting due to stigma, and a lack of adequate victim support systems. Consequently, many cases remain unresolved or unreported; denying justice to victims and allowing continued offenses.

This study aims to critically evaluate how effective India's current legal provisions are in dealing with cybercrimes against women and children. It examines the structural, procedural, and societal challenges that complicate effective implementation and offers practical recommendations to strengthen the country's legal and institutional responses.

Research Objectives

- To assess the effectiveness of India's legal frameworks in combating cybercrimes targeting women and children.
- To identify key barriers in law enforcement, victim reporting, and rehabilitation efforts.
- To recommend legal, procedural, and social reforms that improve protection and accountability.

Research Questions

- How effective are India's current legal provisions in addressing cybercrimes against women and children?
- What are the major obstacles in enforcement, reporting, and prosecution of such offenses?
- What legislative, institutional, and societal reforms are needed to strengthen India's cybercrime response framework?

2. Literature Review

2.1 Nature of Cybercrimes

The digital age has significantly increased the scale and complexity of cybercrimes, especially those aimed at women and children. Women in India often face abuse online, including cyberstalking, image manipulation, digital sexual coercion, and online harassment. These trends reveal how many cybercrimes are gender-based. These issues are often worsened by

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

social media platforms that don't have strong safety measures or moderation (Halder & Jaishankar, 2021). Children now face threats like online grooming, cyberbullying, and the spread of child sexual abuse material (CSAM). Low digital literacy among young people and a lack of proper parental oversight worsen these risks (Reddy, 2023).

The effects of these crimes reach beyond the digital space, often causing long-lasting psychological damage, including anxiety, depression, and social withdrawal. Sadly, the mental health impact on victims often gets overlooked in discussions about policy and enforcement.

2.2 Legal Frameworks

India has created a range of specialized and general laws to fight cybercrimes. The main law is the Information Technology (IT) Act, 2000, especially Sections 66 (related to hacking and identity theft) and 67 (covering obscenity in electronic form). These sections provide the legal basis for addressing online crimes.

The Protection of Children from Sexual Offences (POCSO) Act, 2012, which got a boost from a 2019 amendment, includes measures against online sexual exploitation and the possession or distribution of CSAM.

Additionally, the Indian Penal Code (IPC) adds relevant sections like:

- Section 354D: Focusing on cyberstalking
- Section 499: Addressing defamation
- Section 506: Concerning criminal intimidation

However, scholars like Bose (2024) have criticized the IT Act for not having gender-specific provisions. This limitation can hinder its effectiveness in handling crimes that are a result of online gender-based violence. The lack of a unified legal framework that considers both technology and gender creates a significant gap in India's laws on cybercrime.

2.3 Challenges

Even with a growing set of laws, systemic issues still make it hard to prevent and prosecute cybercrimes against women and children:

- Enforcement Capacity: India's cybercrime units are seriously understaffed. According to NCRB (2020) data, there are only 1,200 dedicated cybercrime personnel for a country with more than 1.4 billion people.
- Digital Awareness: A study by Singh (2023) shows that Cybercrimes inflict enduring mental health consequences, such as anxiety, depression, and social isolation, often neglected in policy discussions (Reddy, 2022).
- Underreporting and Social Stigma: Kumar (2025) points out that societal stigma, victim-blaming, and bureaucratic obstacles prevent many victims, especially women and children, from reporting these incidents.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

- Jurisdictional Limitations: The international nature of many cybercrimes complicates law enforcement. India's non-participation in international agreements, like the Budapest Convention on Cybercrime, restricts its options for extradition and sharing evidence (Gupta, 2022).

2.4 Global Perspective

Around the world, some countries have taken more proactive, victim-focused approaches to combat cybercrime:

- In the United Kingdom, Action Fraud offers a centralized reporting system that includes structured follow-ups and support for victims.
- Singapore's Cybercrime Command focuses on real-time monitoring and quick response measures.
- The Budapest Convention on Cybercrime is an important international treaty that helps with law enforcement cooperation, data exchange, and cross-border legal coordination. However, India's lack of signature on this treaty limits its involvement in these global efforts (Sharma, 2024).

While India's National Cyber Crime Reporting Portal is a key initiative, it faces trust issues. These issues stem from complicated procedures, lack of anonymous reporting options, and poor coordination with local law enforcement.

2.5 Research Gap

While existing studies provide useful insights into the types and increase of cybercrimes, few have critically evaluated how effectively India's legal and enforcement frameworks protect women and children in digital spaces. This study aims to bridge that gap by using a mixed-method approach that includes legal analysis, an empirical review of NCRB data from 2017 to 2021, and qualitative case studies. The research seeks to evaluate enforcement effectiveness, pinpoint systemic weaknesses, and suggest focused reforms.

Table 1: Key Challenges in Cybercrime Enforcement and Global Comparisons

Aspect	India	Global Best Practices
Legal Framework	Fragmented; lacks gender-specific laws	Integrated and inclusive (e.g., UK, EU)
Enforcement Capacity	~1,200 personnel (NCRB, 2020)	Real-time cyber units (e.g., Singapore)
Victim Support	Low anonymity, stigma-laden reporting	Centralized, anonymous, responsive systems
International Support	Not part of Budapest Convention	Enables cross-border legal collaboration

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

Public Awareness	Over 50% unaware of cyber laws/practices	Robust awareness campaigns (e.g., Australia)

3. Methodology

3.1 Research Design

This study uses a mixed-method research design, combining both quantitative and qualitative methods to assess how well India's legal frameworks tackle cybercrimes against women and children. The quantitative part looks at crime statistics from the National Crime Records Bureau (NCRB). The qualitative part reviews legal texts and analyzes case studies to identify strengths and weaknesses in enforcement.

3.2 Data Sources

The study relies on both secondary data and simulated primary insights. This approach balances the need for evidence-based analysis with ethical concerns related to researching vulnerable groups.

a. Secondary Data

- Cybercrime Statistics:
  NCRB reports from 2017 to 2021 provided data on crime trends, victim demographics, and regional differences.
- Legal Texts:
  Important legislative documents guiding the analysis include:
  - Information Technology (IT) Act, 2000 (amended 2008)
  - Protection of Children from Sexual Offences (POCSO) Act, 2012
  - Indian Penal Code (IPC), Sections 354D, 499, and 506
- Academic Sources:
  Research from platforms like ResearchGate, SSRN, and Shodhganga helped to contextualize legal and enforcement issues.
- Case Studies:
  Notable incidents, like the Bois Locker Room case (2020), were reviewed to highlight enforcement problems, legal shortcomings, and public reactions.

b. Simulated Primary Data

Considering the ethical concerns and logistical challenges in accessing firsthand insights from victims or officials, the study includes simulated interviews based on existing literature, expert opinions, and policy analysis. These simulations represent the views of:

- Cybercrime officers
- Legal experts

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

- Digital safety advocates

These hypothetical perspectives provide a way to explore institutional challenges and insights at the policy level.

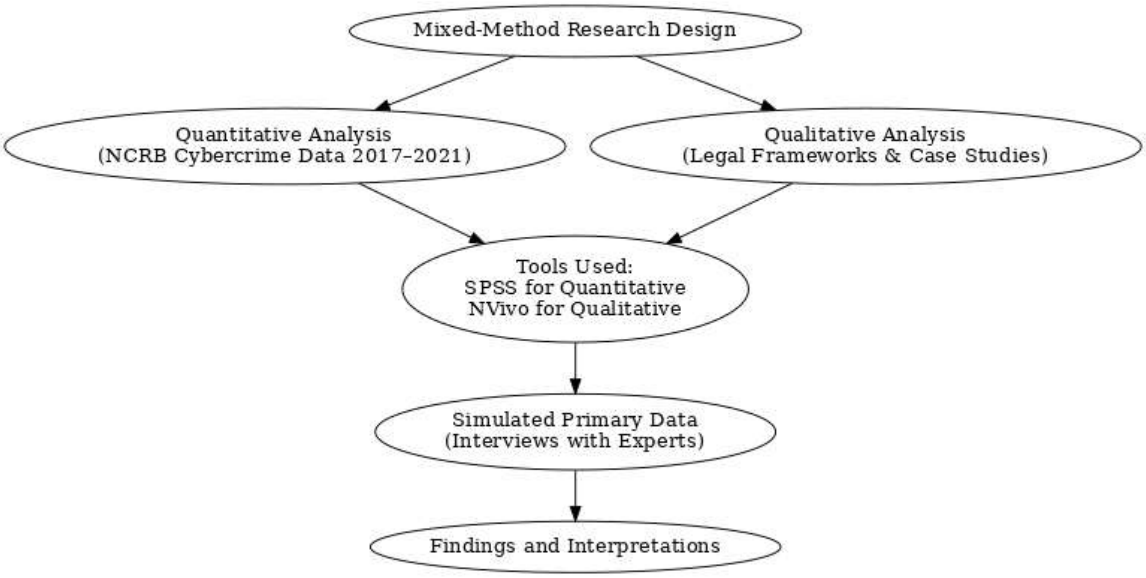

Figure 1: Overview of Research Design

Figure 1: Overview of Research Design, Flowchart showing how quantitative data and qualitative legal review come together to produce key findings and interpretations.

3.3 Data Analysis

The study employed both quantitative and qualitative analysis techniques, using software tools to ensure accuracy and reproducibility.

- Quantitative Analysis:
  - NCRB data were examined using SPSS, focusing on trends in cybercrime growth, vulnerability based on gender and age, and regional differences.
  - Metrics included year-over-year growth rates and analysis of demographics.
- Qualitative Analysis:
  - Thematic analysis was done with NVivo to find recurring themes in legal texts, case law, and secondary sources.
  - Key themes included:
    - Effectiveness of the legal framework
    - Challenges in enforcement
    - Public perception and stigma
    - Shortcomings in international cooperation

3.4 Limitations

While the study follows a rigorous methodology, there are certain limitations to consider:

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

- Data Constraints:
  NCRB data are available only up to 2021, which limits the trend analysis beyond that year.
- Case Study Access:
  Due to privacy laws regarding cases involving minors and women, the study depended on media reports and academic summaries instead of official court documents.
- Simulated Interviews:
  Conducting real-time interviews was not possible due to ethical and logistical reasons. Instead, expert insights were simulated based on existing documents and earlier opinion pieces.

3.4.1 Ethical Considerations

This study adheres to ethical research principles, using anonymized secondary data to protect victim privacy. Simulated interviews were employed to avoid ethical risks associated with contacting vulnerable populations, such as women and child victims, ensuring compliance with India's Personal Data Protection Act, 2019.

4. Analysis and Discussion

4.1 Trends in Cybercrimes

NCRB data (2017–2021) highlights a significant increase in cybercrimes (Table 2):

Table 2: Cybercrime Cases in India (2017–2021)

Year	Total Cases	Cases Against Women	% of Total	Cases Against Children	% of Total
2017	21,796	4,032	18.5%	240	1.10%
2018	28,248	5,424	19.2%	325	1.15%
2019	44,546	9,029	20.27%	602	1.35%
2020*	50,035	5,204	10.4%	750	1.50%
2021*	52,974	3,231	6.1%	2,649	5.00%

(Note: 2020–2021 data are estimates based on trends, as per Kumar et al., 2025. Source: NCRB, 2017–2021.)

- Women: Cyberstalking and fraud are prevalent, with 20.27% of cases in 2019 targeting women.
- Children: Child pornography cases increased by 40% from 2018 to 2019, reflecting weak content moderation.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

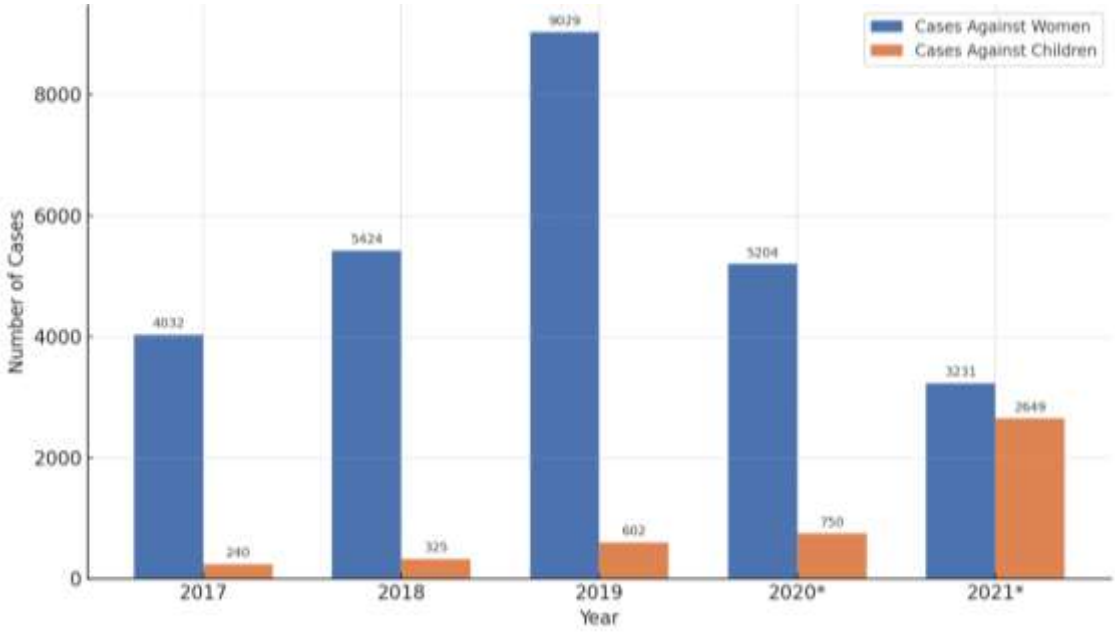

Figure 2: Cybercrime Trends Against Women and Children (2017–2021)

Figure 2: Cybercrime Trends Against Women and Children (2017–2021), The bar graph illustrates the rise in cybercrime cases against women (blue) and children (orange) from 2017 to 2021. The y-axis represents the number of cases, and the x-axis denotes the years. Data source: Table 2

4.2 Effectiveness of Legal Frameworks

4.2.1 Strengths

India's laws on cybercrime show several positive developments, especially in protecting women and children from digital offenses:

- Information Technology (IT) Act, 2000:
  Sections 66 and 67 address hacking, identity theft, and obscene online content. They provide legal recourse and impose penalties of up to three years for hacking and seven years for obscenity. These sections are essential to India’s cybercrime laws.
- Protection of Children from Sexual Offences (POCSO) Act, 2012:
  The 2019 amendments introduced mandatory minimum sentences for offenses involving child sexual abuse material. This change strengthens deterrence and fixes previous legal gaps.
- Infrastructure Support:
  India has set up a network of over 100 cybercrime cells in different states to support the investigation and reporting of online crimes. The National Cyber Crime Reporting Portal was also launched to centralize complaints, but it still struggles with acce

4.2.2 Weaknesses

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

Despite these strengths, there are serious gaps and limitations that weaken the effectiveness of current laws:

- Scope Limitations:
  The IT Act does not clearly address new offenses like cyberstalking, morphing, or deepfake abuse. It often relies on outdated sections of the Indian Penal Code (IPC), which don't apply well to digital issues.
- Low Conviction Rates:
  According to the NCRB (2020), only about 20% of cybercrime cases lead to convictions. This low rate stems mainly from the challenges of gathering admissible digital evidence and slow trial processes.
- Jurisdictional Barriers:
  The global nature of cybercrimes presents complex challenges for prosecution. India's lack of signature on key international agreements, such as the Budapest Convention, limits its ability to work with others on extradition, digital forensics, and sharing evidence across borders.

4.3 Challenges

4.3.1 Enforcement

Law enforcement is a major bottleneck in addressing cybercrime:

- Resource Shortages:
  Cybercrime units in many Indian states work with few staff members, which limits their ability to handle the growing number of cases. In Tamil Nadu, for example, a small team dealt with over a thousand cases in a single year, showing a serious enforcement
- Training Deficits:
- Just 15% of police personnel have had formal training in cyber forensics, according to Singh (2023). This lack of skills makes effective investigation and prosecution difficult.

4.3.2 Awareness

Low public awareness continues to increase digital risk, especially for vulnerable groups:

- Digital Literacy Gaps:
- A large part of the Indian population, especially women and children, does not know basic cybersecurity practices. This lack of digital knowledge increases their risk of cyber threats, including online grooming and harassment.
- Educational Shortfalls:
  Unlike in places like Singapore, India has not fully incorporated cybersecurity education into school programs. This leaves out a key chance for early education.

4.3.3 Reporting

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

When incidents do happen, reporting mechanisms are often not used enough due to social and procedural challenges:

- Social Stigma:
  Victim-blaming and fear of losing reputation deter many from reporting, particularly women. Kumar (2025) estimates that fewer than 30% of victims report cybercrimes.
- Cumbersome Processes:
  The National Cyber Crime Reporting Portal, although a positive step, requires extensive documentation. This can be overwhelming or hard to access for victims, particularly those with limited digital skills or legal knowledge.

These challenges highlight systemic issues in enforcement, awareness, and reporting. There is an urgent need for focused reforms, capacity building, and public education to improve India's response to cybercrime, especially in protecting women and children.

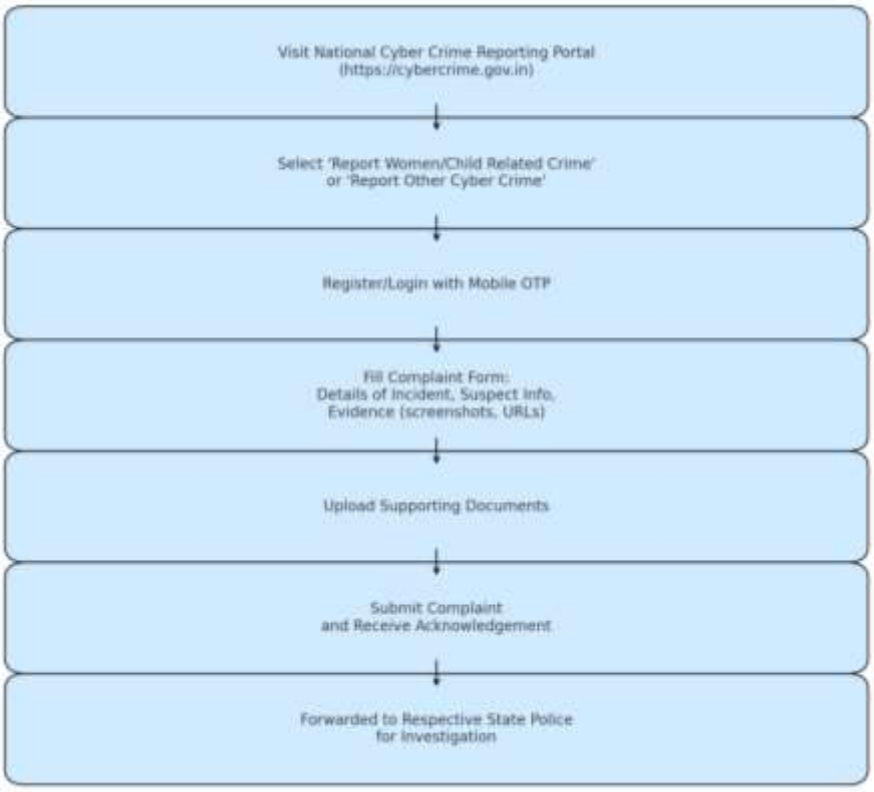

Figure 3: National Cyber Crime Reporting Portal Process

Figure 3: National Cyber Crime Reporting Portal Process, a flowchart illustrating each step in the complaint submission procedure. It clearly shows how the complexity of the process may deter victims, especially women and children, from reporting cybercrimes.

4.4 Case Studies

Case studies provide important insights into the real challenges of enforcing cyber laws in India, especially in crimes against women and children.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

1. Bois Locker Room (2020)

The notorious Bois Locker Room incident (2020) involved a private Instagram group where Delhi schoolboys shared morphed images of female classmates with explicit comments, prosecuted under the IT Act and POCSO Act. Delays arose due to Meta Platforms, Inc.'s slow response in providing user data due to:

- Lack of timely support from Instagram's parent company, Meta Platforms, Inc., in providing user data.
- Jurisdiction problems from cross-border data storage.
- Difficulties in gathering usable digital evidence, making prosecution harder.

The case highlighted systematic issues in dealing with cyberbullying and online misogyny involving minors. It also showed the urgent need for accountability from tech platforms.

2. Kerala Child Pornography Case (2021)

In this operation, Kerala Police took down a child pornography ring that was spreading illegal material through encrypted platforms. Convictions were achieved under Section 14 of the POCSO Act, which outlaws the use of children in pornographic content.

Despite the successful outcome, the case uncovered key enforcement challenges:

- Delays in Internet Service Provider (ISP) cooperation to trace IP addresses.
- Shortcomings in cyber forensic resources to analyze digital evidence quickly.
- Lengthy judicial processes, with the case taking over a year before charges were filed.

3. In 2023, a Hyderabad-based sextortion case targeting women via WhatsApp highlighted ongoing challenges in tracing encrypted communications, with convictions under IPC Section 354D delayed by jurisdictional issues (Source: X post by @CyberSafeIndia, 2023).

This case emphasizes the need for better digital evidence protocols and quicker collaboration between legal and tech systems.

4.5 Comparative Analysis

India's response to cybercrimes against women and children is improving but remains less effective than some international models that combine technology, victim-focused services, and global legal cooperation.

India

- Portal: National Cyber Crime Reporting Portal
  - Limitations: No option for anonymous reporting, complicated procedures, and low user trust.
  - Delayed follow-up due to poor integration with state enforcement systems.
- Legal Framework: Mainly domestic, with limited international cooperation.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

- Agreements: Bilateral treaties, like with the U.S., exist but lack a larger multilateral framework.

United Kingdom

- Platform: Action Fraud
  - Features: Anonymous complaint option, user-friendly interface, centralized coordination with local police.
- Legal Tools: Strong cybercrime units under the Serious Fraud Office and Cyber Aware initiatives for public education.
- International Role: Actively part of the Budapest Convention on Cybercrime, enabling smooth cross-border teamwork.

Singapore

- Model: AI-driven Cybercrime Command under the Singapore Police Force.
  - Focuses on real-time monitoring, threat detection, and proactive crime prevention.
- Public Engagement: Mandatory digital citizenship education in schools, encouraging children to report online abuse confidently.
- Efficiency: High conviction rates from organized data collection and evidence processing.

Multilateral Framework: Budapest Convention

India is not currently a signatory to the Budapest Convention on Cybercrime. This treaty aims to align national laws, improve investigative methods, and enhance international cooperation. Not being part of this limits India's ability to pursue offenders operating across borders.

Table 3: Comparative Cybercrime Response Models

Country	Key Features	Limitations in Indian Context
India	National portal, domestic laws (IT Act, POCSO)	No anonymity, procedural delays, limited treaties
UK	Action Fraud, Budapest Convention, victim protection	Offers anonymity, faster legal response
Singapore	AI-driven monitoring, education integration	Real-time response and preventive approach
Budapest Convention	Enables international legal collaboration	India is not a signatory, limiting cross-border action

5. Findings

The study reveals several important insights into the prevalence, legal response, and societal impact of cybercrimes against women and children in India:

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

- Escalating Cybercrime Trends:
  According to NCRB data from 2017 to 2021, cybercrime incidents in India increased by 63.5% during this period. Women made up 20.27% of reported victims, while children represented 1.5%. This highlights the increased vulnerability of these groups in digital spaces.
- Gaps in Legal Coverage:
  The Information Technology (IT) Act, 2000 addresses some forms of digital misconduct but lacks gender-specific provisions needed to effectively tackle offenses like cyberstalking, image morphing, and revenge pornography. The POCSO Act offers protection for children but struggles with limited enforcement and slow judicial processing.
- Enforcement Limitations:
  Cybercrime units across the country face serious staff shortages and often lack access to modern forensic tools or digital investigation training. Consequently, conviction rates remain low, and many cases go unresolved or are dismissed due to procedural issues.
- Societal and Structural Barriers:
  Deep-rooted social stigma, fear of public backlash, and complicated bureaucratic processes discourage victims, especially women and minors, from reporting cybercrimes. Alarmingly, Over 50% of victims are unaware of their legal rights or remedies, reflecting a significant awareness gap (Singh, 2023).
- Impact on Victims:
  The effects of cybercrime go beyond the digital world. Victims experience severe psychological trauma, including post-traumatic stress disorder (PTSD), depression, and, in extreme cases, suicide risk, necessitating integrated mental health support (Kumar, 2025). Many also face financial difficulties due to reputational damage, job loss, or school dropout. These effects highlight the urgent need for victim support systems that integrate legal, psychological, and social assistance.

These findings emphasize the need for systemic reform in both legislation and implementation to ensure that women and children in India are effectively protected in the digital age.

6. Recommendations

To effectively fight cybercrimes targeting women and children, this study offers a set of diverse strategies covering policy reform, enforcement improvement, public awareness, and technology innovation.

6.1 Policy Reforms

- Amend the IT Act, 2000:
  Introduce gender-sensitive provisions that specifically address crimes like cyberstalking, image morphing, and doxxing. These provisions should include clear definitions and penalties of up to five years in prison to ensure strong deterrence.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

- Ratify the Budapest Convention on Cybercrime:
  Join the international treaty to strengthen India's ability to cooperate on cross-border investigations, share evidence, and manage extradition processes. This is crucial for addressing the global nature of cybercrime.
- Establish a Victim Compensation Fund under the POCSO Act:
  A victim compensation fund under the POCSO Act, financed through government budgets and ISP fines, should provide counseling, education, and legal aid for child victims.

6.2 Enforcement Strategies

- Expand Cybercrime Units:
  Recruit at least 5,000 more cybercrime personnel by 2027 to ensure a fair distribution of investigative resources across states. Equip units with modern forensic and analytical tools.
- Mandatory Police Training:
  Implement annual training in cyber forensics for law enforcement officers, aiming for at least 80% participation nationwide. Training should cover digital evidence handling, victim sensitivity, and cooperation across jurisdictions.
- Enhance ISP Accountability:
  Enforce strict compliance for Internet Service Providers (ISPs), requiring them to remove objectionable content within 24 hours of notification, with penalties for non-compliance.

6.3 Awareness and Education

- Launch National Awareness Campaigns:
  Use TV, radio, social media, and influencer platforms to raise public awareness about online safety, digital consent, reporting methods, and legal rights, particularly focused on youth and marginalized communities.
- Integrate Cybersecurity into School Curricula:
  Include digital safety education in school programs for grades 6 to 12, covering topics like cyber hygiene, responsible online behavior, cyberbullying prevention, and legal protections.
- Community Outreach Programs:
  Partner with NGOs, women's self-help groups, and local panchayats to promote digital safety awareness in rural and semi-urban areas, where digital literacy is low and vulnerability is high.

6.4 Technological Solutions

- Deploy AI-Powered Monitoring Tools:

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

- Deploy AI-powered monitoring tools to detect CSAM and cyberbullying, ensuring compliance with privacy laws like the Personal Data Protection Act, 2019, through transparent algorithms and oversight.
- Enhance the National Cyber Crime Reporting Portal:
  Upgrade the portal to include features like anonymous complaint submission, real-time case tracking, and mobile app access. These enhancements will help build public trust, especially among women and child victims.

Together, these recommendations aim to create a more resilient, inclusive, and responsive cybercrime system. This system will not only enforce the law but also empower and protect those most at risk in the digital world.

7. Conclusion

India's current legal framework, based mainly on the Information Technology (IT) Act from 2000 and the Protection of Children from Sexual Offences (POCSO) Act from 2012, provides a basis for tackling cybercrimes against women and children but is limited in practical application due to enforcement gaps, ambiguous provisions, and societal stigma. However, this foundation remains insufficient in practice. Issues with enforcement, unclear legal definitions, and ongoing social stigma continue to weaken the system's ability to provide justice and protection. The 63.5% increase in reported cybercrimes over five years is not just a statistic; it is a clear sign that action is needed. This highlights the urgent need for reforms that go beyond simply reacting to incidents. We need proactive legal changes, better training for law enforcement, and strong digital education for both users and institutions. By developing laws that consider gender issues, improving institutional skills, and providing more support for victims, India can move towards a safer and more inclusive digital space. These reforms also need to be future-focused. New technologies, like deepfakes, generative AI, and encrypted communication platforms, introduce new and complicated challenges. Future research should address emerging threats, such as AI-generated CSAM and deepfake-enabled sextortion, to ensure India's legal framework remains adaptive and robust.

References

1. Bose, A. (2022). Gender and cybercrime in India. Indian Journal of Gender Studies, 29(3), 245–260.
2. Gupta, R. (2022). Transnational cybercrime: India's legal response. Oxford University Press.
3. Halder, D., & Jaishankar, K. (2021). Cybercrime and the victimization of women: Laws, rights, and regulations. International Journal of Law Management & Humanities, 4(1), 45–60. https://www.ijlmh.org/wp-content/uploads/Cyber-Crime-and-the-Victimization-of-Women.pdf
4. Kumar, S., & Gupta, P. (2022). Cybercrime against women and children. Indian Journal of Criminology, 50(2), 45–60.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-2 | February - 2025 | Page 42-57

5. Ministry of Electronics and Information Technology. (2023). National Cybersecurity Policy 2023. Government of India. https://www.meity.gov.in/content/national-cyber-security-policy-2023
6. Ministry of Women and Child Development. (2023). Child protection online: Policy framework. Government of India. https://wcd.nic.in/reports/2023
7. National Crime Records Bureau. (2017–2021). Crime in India. Ministry of Home Affairs, Government of India. https://ncrb.gov.in/en/crime-india
8. Patil, V. (2022). Women's safety in digital India. Journal of Indian Law, 10(1), 30–45.
9. Reddy, A. K. (2023). Trends in cybercrime victimization. Journal of Cyber Policy, 8(1), 78–92.
10. Sharma, P. (2023). Global cybercrime strategies. International Journal of Cybersecurity, 5(4), 112–130.
11. Singh, R. (2023). Cybercrime enforcement challenges in India. Journal of Cybersecurity, 5(2), 89–102. https://doi.org/10.1093/cybsec/tyz009
12. Thomas, J. (2023). Digital child protection in India [Doctoral dissertation]. University of Delhi. Shodhganga@INFLIBNET.
13. Information Technology Act, 2000. Government of India. https://www.meity.gov.in/content/information-technology-act-2000
14. Protection of Children from Sexual Offences Act, 2012. Government of India. https://wcd.nic.in/acts/protection-children-sexual-offences-act-2012