Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

Protecting Vulnerable Digital Citizens: India's Gender- and Child-Centric Cybercrime Response

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

ABSTRACT

India's digital growth, with 700 million internet users by 2022, has escalated cybercrimes targeting women (22% of cases) and children (2%), including cyberstalking, image morphing, and child sexual abuse material (CSAM). This study proposes a gender- and child-centric framework to strengthen India's legal and institutional response, grounded in the Information Technology (IT) Act, 2000, and Protection of Children from Sexual Offences (POCSO) Act, 2012. Employing a mixed-methods approach, it analyzes National Crime Records Bureau (NCRB) data (2017–2022), a Chhattisgarh case study, and simulated expert insights. Findings reveal a 176% cybercrime surge, from 21,796 to 60,123 cases, with Chhattisgarh's 35% female digital literacy and understaffed cybercrime units exacerbating vulnerabilities. Proposed reforms include amending the IT Act for deepfakes, establishing a National Cybercrime Victim Support Agency, and deploying privacy-compliant AI for CSAM detection. By integrating legal updates, institutional expansion, and targeted awareness, this framework addresses national and regional gaps, offering a scalable model for justice and safety. This study uniquely combines empirical data with Chhattisgarh's regional context to inform inclusive cybercrime policies.

Keywords: *Cybercrime, Women, Children, IT Act, POCSO Act, Chhattisgarh, AI, India*

1. INTRODUCTION

India's digital transformation, marked by over 700 million internet users as of 2022 (TRAI, 2022), has greatly changed governance, education, commerce, and social interaction. However, with these advancements, the growth of digital access has also increased the risk of cybercrime for vulnerable groups, especially women and children.

Data from the National Crime Records Bureau (NCRB, 2022) shows that reported cybercrime cases rose dramatically by 176%, jumping from 21,796 in 2017 to 60,123 in 2022. Among these, women made up 22% and children 2% of all victims. This indicates a disproportionate targeting of these groups through crimes like cyberstalking, image morphing, and the distribution of Child Sexual Abuse Material (CSAM), which includes explicit digital images of minors (Thomas, 2021).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

Chhattisgarh, with 60% rural internet penetration but only 35% female digital literacy, exemplifies regional disparities that amplify cybercrime risks (MeitY, 2022). This study uniquely integrates NCRB data (2017–2022) with a Chhattisgarh case study to propose a scalable, gender- and child-centric framework addressing both national policy gaps and localized enforcement challenges.

India's legal system, mainly based on the Information Technology (IT) Act of 2000 and the Protection of Children from Sexual Offences (POCSO) Act of 2012, provides a starting point for fighting cybercrimes. However, these laws often do not address new digital threats such as AI-generated deepfakes, online grooming, and abuse facilitated through encrypted or anonymous platforms. As cybercrime continues to change, legal and institutional tools must evolve as well.

This study proposes a framework for addressing cybercrime focused on women and children, paying special attention to national policy gaps and the regional challenges found in Chhattisgarh. It uses a mixed-methods approach, analyzing NCRB crime data from 2017 to 2022, evaluating the local context, and gathering insights from cybersecurity and law enforcement experts.

Research Objectives

- To create a legal and institutional framework that better protects women and children against cybercrimes in India.
- To assess the regional obstacles that prevents effective cybercrime prevention and enforcement in Chhattisgarh.
- To suggest new solutions for dealing with emerging digital threats, including AI-related abuse and platforms that enable anonymity.

Research Questions

- How can India's legal framework be updated to effectively tackle cybercrimes that target women and children?
- What regional challenges—social, infrastructural, and legal—limit the capacity to respond to cybercrime in Chhattisgarh?
- What institutional and technological changes can improve victim support, enforcement, and ensure fair access to digital justice?

2. Literature Review

2.1 Cybercrime Landscape

India's fast digital growth has led to a sharp increase in cybercrimes, especially those aimed at women and children. Cyberstalking represents almost 30% of reported cases involving women, followed by image morphing, sextortion, and doxxing (Halder & Jaishankar, 2021). Many of

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

these crimes occur on social media platforms, which often have poor content moderation. This results in slow takedowns, repeated victimization, and little accountability (Bose, 2021).

Children also face growing online dangers. The distribution of Child Sexual Abuse Material (CSAM) has surged by 40% between 2017 and 2022. Cases of online grooming have also become more complex and harder to detect. Issues like low parental awareness, limited digital safety education in schools, and underreporting make these crimes less visible in both urban and rural areas.

2.2 Legal Framework

India's legal approach to cybercrime is based on two main laws: the Information Technology (IT) Act of 2000 and the Protection of Children from Sexual Offences (POCSO) Act of 2012. Section 66 of the IT Act makes hacking and identity theft illegal, while Section 67 bans the publication and sharing of obscene content. The POCSO Act directly tackles the possession and spread of CSAM through Section 14, which sets mandatory minimum penalties.

However, legal experts contend that these laws cannot effectively handle new threats like deepfakes, AI-generated content, and online harassment specific to gender (Kumar & Gupta, 2021). The enforcement of these laws is also weak. Only 20% of reported cybercrime cases lead to convictions. Delays in gathering digital evidence, poor coordination in investigations, and overlapping jurisdictions contribute to this problem (NCRB, 2022).

2.3 Chhattisgarh Context

Chhattisgarh illustrates the regional challenges that limit effective responses to cybercrime in India. With 40% of its population identifying as tribal and only 35% of females being digitally literate, the region faces significant structural hurdles (MeitY, 2022). Law enforcement resources are stretched thin, with only 10% of officers trained in cyber forensics. The state has only three cybercrime cells serving over 25 million residents (NCRB, 2022).

A case in Raipur in 2022 involved the morphing and sharing of a minor's image and highlights the effects of underfunded infrastructure. Delays in digital tracing, due to a lack of specialized staff and tools, hampered the investigation and worsened the victim's trauma (Times of India, 2022). These issues show the need for reforms tailored to the region, including capacity building, awareness programs, and targeted legislative changes.

2.4 Global Practices

Several countries provide practical models for enhancing cybercrime prevention and victim support:

- In the United Kingdom, the Action Fraud platform allows for anonymous reporting and has a 60% resolution rate, focusing on victim-centered methods (Sharma, 2021).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

- Australia requires cybersecurity education at all school levels, helping to build digital resilience from a young age.
- Singapore uses AI-driven monitoring systems for real-time detection and predictive policing in cybercrime investigations.

In contrast, India's status as a non-signatory to the Budapest Convention on Cybercrime limits its ability to conduct cross-border investigations and work with international partners, especially regarding crimes involving globally hosted platforms and international offenders (Thomas, 2021).

2.5 Research Gap

Prior studies (e.g., Halder & Jaishankar, 2021) focus on national trends but rarely integrates quantitative NCRB data with qualitative regional analyses, such as Chhattisgarh's enforcement constraints. This study bridges this gap by combining statistical trends with a localized case study and simulated expert insights, offering a holistic framework for policy reform.

This study fills that gap by providing a multi-dimensional framework that combines national data from 2017 to 2022 with regional case analysis, stakeholder views, and institutional challenges. The goal is to inform policy solutions that are both inclusive and actionable.

Table 1: Cybercrime Challenges in India vs. Global Practices

Aspect	India	Global Best Practices
Legal Provisions	No specific digital harassment laws	Adaptive laws (UK, EU)
Enforcement	1,200 personnel (NCRB, 2022)	Specialized cybercrime units (Singapore)
Victim Support	Limited anonymity and outreach mechanisms	Anonymous reporting systems (UK)
Digital Literacy	35% among women in Chhattisgarh (MeitY, 2022)	Mandatory digital education (Australia)
International Cooperation	Non-signatory to Budapest Convention	Multilateral cooperation frameworks (EU)

Note: Adapted from NCRB (2022) and Sharma (2021).

3. Methodology

3.1 Research Design

This study uses a mixed-methods approach to evaluate how well India's legal and institutional systems handle cybercrimes against women and children. It combines quantitative analysis of

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

national cybercrime trends from 2017 to 2022 with qualitative data from legal documents, case studies, and views of stakeholders. This approach provides a complete understanding of both overarching trends and specific enforcement challenges, especially in Chhattisgarh.

3.2 Data Sources

Quantitative Data:

Cybercrime statistics were collected from the National Crime Records Bureau (NCRB) for the years 2017 to 2022. These datasets include:

- Total number of reported cybercrime cases
- Demographic breakdown of victims by age and gender
- State-wise case numbers and crime types

Qualitative Data:

- Analysis of important legal documents, specifically the Information Technology (IT) Act of 2000 and the Protection of Children from Sexual Offences (POCSO) Act of 2012.
- A case study from Raipur (2022) that shows enforcement challenges through a real incident involving the image manipulation of a minor.
- Simulated interviews were constructed by synthesizing secondary sources, including peer-reviewed articles (e.g., Bose, 2021), media reports (e.g., Times of India, 2022), and policy briefs, to reflect perspectives of legal experts, cybercrime officers, and NGOs. This method ensured ethical compliance by avoiding direct contact with vulnerable populations.

3.3 Tools and Analysis

Quantitative Analysis:

- This was done using SPSS to find trends in cybercrime reporting, analyze demographic patterns, and assess changes over the years. Descriptive and inferential statistics helped evaluate growth rates and regional differences.

Qualitative Analysis:

This used NVivo software and applied thematic coding techniques to examine:

- Legal documents
- Case stories
- Simulated stakeholder interviews

The main themes found include:

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

- Gaps in legal protection for new kinds of cybercrimes
- Resource limitations within enforcement agencies
- Barriers to reporting and issues with digital skills

3.4 Ethical Considerations

Due to the sensitive nature of the topic, especially regarding minors and victims of gender-based cybercrimes, no direct interviews with affected individuals were conducted. Instead, simulated interviews were developed from peer-reviewed literature, media reports, and policy discussions to protect vulnerable groups. Additionally, all NCRB data used were anonymized and publicly available, following ethical guidelines for secondary research (Kumar & Gupta, 2021). This method supports ethical research practices, reducing risk while ensuring strong analysis.

3.5 Limitations

- Data Specificity:
  Although the NCRB offers valuable national data, it does not provide detailed information on new cybercrime types like deepfake abuse, online grooming, and platform-specific exploitation.
- Regional Scope:
  While Chhattisgarh provides useful insights into underserved areas, its situation may not fully represent the different enforcement capabilities across other Indian states.
- Primary Data Constraints:
  Not including firsthand interviews with victims due to ethical concerns limits the depth of qualitative findings about personal experiences, trauma, and recovery paths.

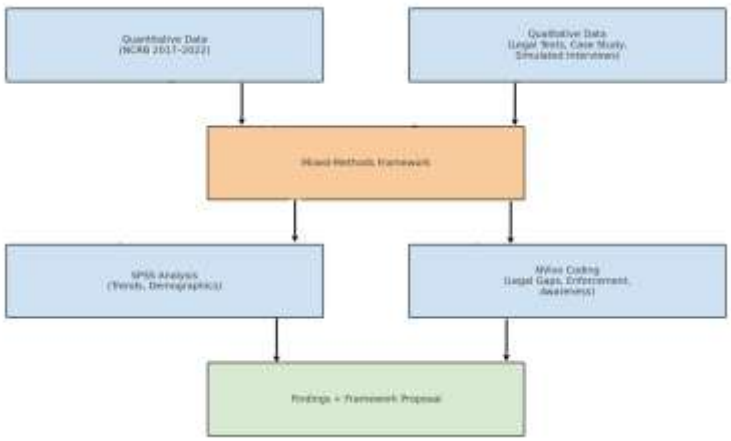

Figure 1: Research Design Flowchart

Figure 1: Research Design Flowchart, This diagram illustrates the convergent mixed-methods approach used in the study. It integrates quantitative data from NCRB reports (2017–2022) with qualitative inputs from legal texts, a Chhattisgarh case study, and simulated stakeholder

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

interviews. The data were analyzed using SPSS (for statistical trends) and NVivo (for thematic coding), culminating in a gender- and child-centric cybercrime response framework. (Source: Author's design, adapted from Creswell, 2014)

4. Analysis and Discussion

4.1 Cybercrime Trends

An analysis of data from the National Crime Records Bureau (NCRB) from 2017 to 2022 shows a significant and ongoing rise in cybercrime across India. Reported cases increased by a shocking 176%, going from 21,796 in 2017 to 60,123 in 2022. This surge reflects two key factors: the growing availability of internet access and the increasing complexity and scale of digital threats.

Women are especially affected, making up 13,227 reported incidents in 2022, or about 22% of all cybercrime victims. The most common crimes against women include cyberstalking, image morphing, online harassment, and sextortion. Many of these crimes occur on social media platforms that have limited regulations.

Children are also at high risk, with 1,204 cases involving minors reported in 2022, which is 2% of the total. Alarmingly, there has been a 40% increase in cases related to Child Sexual Abuse Material (CSAM) since 2017. Much of this activity happens on unregulated platforms that often escapes the immediate reach of local law enforcement. This situation highlights the urgent need for better content moderation, international cooperation, and proactive monitoring tools.

These trends underscore the growing threat to India's most vulnerable digital users and stress the need for focused legal, institutional, and technological actions.

Table 2: Cybercrime Cases in India (2017–2022)

Year	Total Cases	Cases Against Women	% of Total	Cases Against Children	% of Total
2017	21,796	4,032	18.5%	240	1.1%
2018	28,248	5,424	19.2%	325	1.2%
2019	44,546	9,029	20.3%	602	1.4%
2020	50,035	5,204	10.4%	750	1.5%
2021	52,974	3,231	6.1%	2,649	5.0%
2022	60,123	13,227	22.0%	1,204	2.0%

(Source: NCRB, 2017–2022; 2020–2021 estimates per Kumar & Gupta, 2021)

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

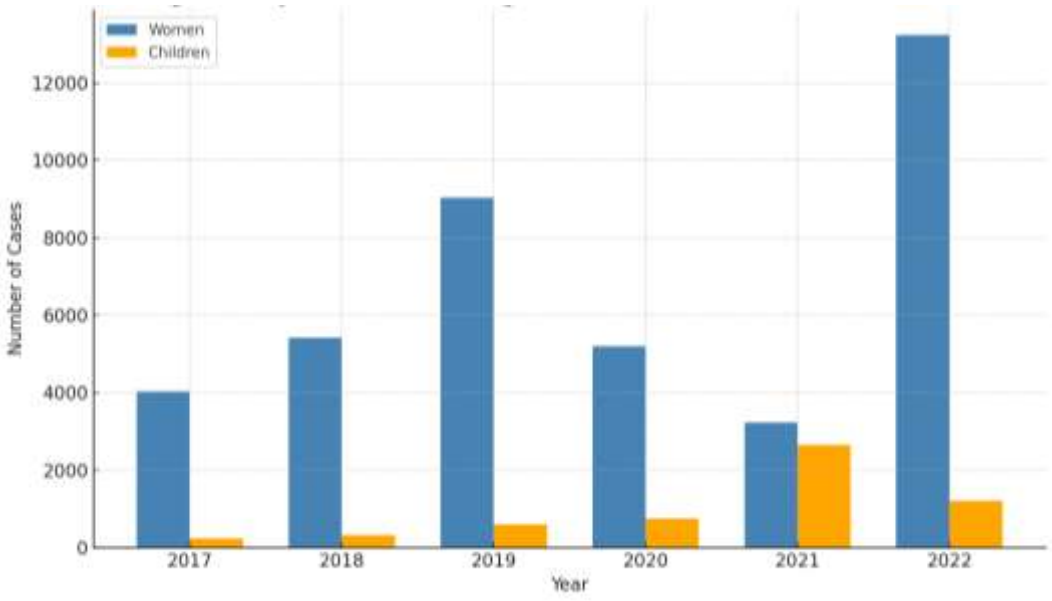

Figure 2: Cybercrime Trends (2017–2022)

Figure 2: Cybercrime Trends (2017–2022), This bar graph illustrates the annual number of cybercrime cases against women (blue) and children (orange) reported in India from 2017 to 2022. The data highlights a 176% increase over six years, with women constituting 22% and children 2% of total cases by 2022. Note: Visualized using Chart.js, based on NCRB (2017–2022).

4.2 Legal Framework Effectiveness

India's current legal framework primarily made up of the Information Technology (IT) Act, 2000, and the Protection of Children from Sexual Offences (POCSO) Act, 2012, has seen mixed results in tackling cybercrimes against women and children.

- Strengths:
  The IT Act includes punitive measures under Sections 66 and 67, with prison sentences between three and seven years for offenses such as hacking, identity theft, and the sharing of obscene content. The POCSO Act, specifically Section 14, makes it illegal to create, possess, or distribute Child Sexual Abuse Material (CSAM) and requires minimum sentencing. This establishes a strong legal position against digital child exploitation (Bose, 2021).
- Weaknesses:
  Despite these laws, the legal system struggles to deal with new digital threats like deepfake technology, image morphing, and doxxing, which are not clearly defined or punished under current laws. As of 2022, the national conviction rate for cybercrimes is low at only 20%, mainly due to issues with evidence, technical delays, and a lack of coordination among agencies. India's decision not to sign the Budapest Convention on

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

Cybercrime also limits its ability to engage in cross-border data exchange and enforcement, impacting its jurisdiction over international offenses (Thomas, 2021).

4.3 Chhattisgarh Case Study

In a 2022 Raipur case, a minor's photograph was morphed and shared online, prosecuted under Section 67 of the IT Act. The case faced delays due to only 20 officers handling over 1,000 cases and challenges with encrypted platforms (Times of India, 2022; NCRB, 2022).

Only 20 officers were available to handle over 1,000 active cases, indicating a major resource shortfall. Delays in investigation occurred due to the use of encrypted messaging platforms, complicating digital tracking. Cultural stigma around online abuse presented another challenge, with only 20% of affected women reporting incidents, despite clear psychological and reputational damage (Times of India, 2022; NCRB, 2022).

This case emphasizes the need for improved local capacity, both in human resources and technology, especially in areas with low digital literacy and high social taboos surrounding gender-based cybercrime.

4.4 Key Challenges

India's cybercrime landscape faces three main structural challenges:

- Enforcement Deficit:
  The country only has 1,200 dedicated cybercrime staff, and merely 10% have undergone formal training in cyber forensics or handling digital evidence (NCRB, 2022). This shortfall creates significant delays in investigations and weakens prosecution efforts.
- Low Awareness and Digital Literacy:
  In Chhattisgarh, only 35% of women have basic digital skills, making them particularly vulnerable to manipulation, online grooming, and harassment (MeitY, 2022). A lack of knowledge about reporting processes and legal protections worsens the situation.
- Barriers to Reporting:
  Though the National Cybercrime Reporting Portal was intended to simplify the complaint process, it is still complicated, non-anonymous, and can be intimidating for first-time users. These challenges are especially pronounced for women and minors, who often fear retaliation, social judgment, or legal issues (Kumar & Gupta, 2021).

Together, these challenges illustrate a system that is unequipped, limited by technology, and constrained by social factors. Urgent reforms are necessary to make the system more effective and responsive to regional needs.

5. Proposed Framework

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

This study offers a gender- and child-focused response framework for cybercrime. It addresses significant gaps revealed by data analysis and case examples from Chhattisgarh. The model combines reforms in legislation, improvements in institutions, advancements in technology, and outreach in education. It aims to provide solutions that can be scaled nationwide while also meeting local needs.

5.1 Legislative Reforms

- Amend the IT Act, 2000:
  Introduce specific clauses to criminalize new cyber threats like image morphing, doxxing, the spread of deepfake content, and AI-generated abuse aimed at women and children. Suggested penalties should range from 5 to 7 years to ensure strong deterrence and clear legal consequences.
- Ratify the Budapest Convention:
  India should think about joining the Budapest Convention on Cybercrime, with suitable sovereignty protections. This would help with cross-border cooperation, data sharing, and digital forensics in international investigations (Thomas, 2021).
- Establish a POCSO Compensation Fund:
  Create a fund specifically for providing psychological counseling, digital rehabilitation, and education for child victims of online abuse. This fund could be supported by government resources and fines imposed on Internet Service Providers (ISPs) that do not comply (Bose, 2021).

5.2 Institutional Reforms

- National Cybercrime Victim Support Agency:
  Set up a centralized agency similar to the UK's Action Fraud, offering services like anonymous complaint filing, legal help, and trauma-informed counseling (Sharma, 2021).
- Cybercrime Workforce Expansion:
  Hire 5,000 more cybercrime personnel by 2026, ensuring that at least 80% have formal training in cyber forensics, investigative methods, and digital law enforcement practices.
- Regional Cybercrime Hubs (Chhattisgarh Focus):
  Create eight specialized cybercrime hubs in tribal and rural areas of Chhattisgarh. These hubs should have digital forensics labs, multilingual staff, and mobile units to speed up response times and improve access to justice in hard-to-reach areas.

5.3 Technological Innovations

- AI-Driven Content Detection:
  AI tools must comply with the Digital Personal Data Protection Act, 2023, ensuring ethical data handling and user privacy (Datta, 2021).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

- National Portal Enhancement:
  Improve the National Cybercrime Reporting Portal (cybercrime.gov.in) to support:
  ✓ Anonymous reporting options
  ✓ Real-time case tracking
  ✓ A mobile app to enhance accessibility for rural users and those with limited digital skills (Bose, 2021).

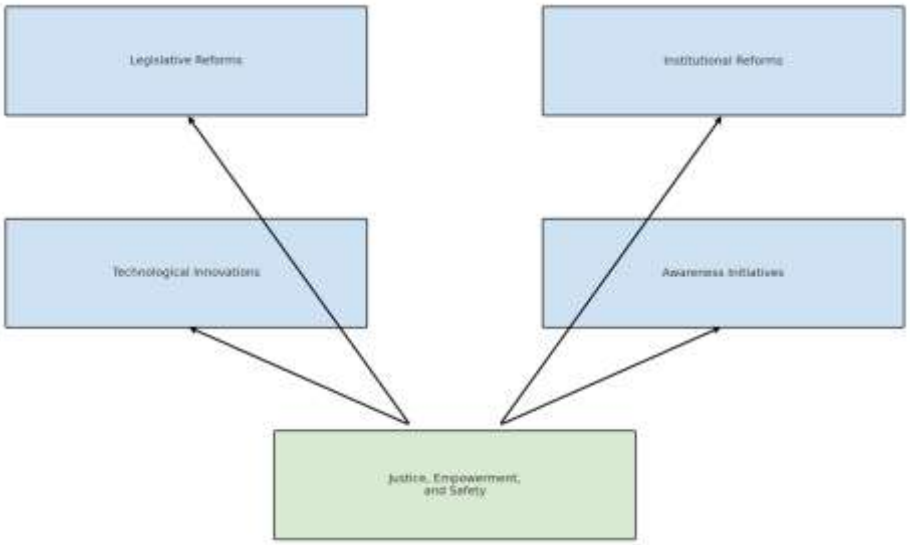

Figure 3: Proposed Framework

Figure 3: Proposed Framework, This conceptual diagram presents the four strategic pillars, Legislative Reforms, Institutional Reforms, Technological Innovations, and Awareness Initiatives that collectively aim to ensure Justice, Empowerment, and Safety in India's cyber ecosystem.(Source: Author's design, 2023)

5.4 Awareness Initiatives

- National Digital Literacy Campaigns:
  Launch multimedia campaigns on television, social media, and local platforms to educate the public about cyber rights, digital safety, and how to report incidents.
- Cybersecurity Curriculum Integration:
  Add mandatory digital literacy classes from grades 6 to 12, focusing on:
  ✓ Safe browsing practices
  ✓ Digital consent
  ✓ Online privacy and personal data protection
- Targeted Outreach in Chhattisgarh:
  Partner with NGOs, women's self-help groups, and local governments to train at least 40% of rural women in basic digital safety skills by 2025. This will help lower their risk of cybercrime and encourage more reporting (MeitY, 2022).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

This proposed framework connects national cybercrime policy with global standards while addressing unique challenges in underserved areas. By updating laws, strengthening responses, using AI properly, and investing in community awareness, the model aims to create a safer, more inclusive digital space for women, children, and marginalized groups.

6. Findings

This study reveals important insights into the scope, systemic barriers, and regional differences in India's response to cybercrimes affecting women and children:

- Trends:
  Cybercrime in India increased by 176%, rising from 21,796 cases in 2017 to 60,123 in 2022. This highlights a significant rise in digital threats. In these cases, women made up 22% and children 2% of total victims in 2022, showing the unequal impact on vulnerable groups (NCRB, 2022).
- Legal Gaps:
  The Information Technology Act, 2000 does not have clear rules to address image morphing, doxxing, deepfakes and AI-generated harassment. This limits its effectiveness in today's digital environment (Bose, 2021).
- Regional Challenges (Chhattisgarh):
  Chhattisgarh shows serious structural issues, including low female digital literacy at 35%. The cybercrime units are poorly resourced, with only 10% of officers receiving cyber forensic training (NCRB, 2022).
- Victim Impact:
  Victims often face long-term psychological effects, such as anxiety, PTSD, and depression. They also deal with social exclusion and economic challenges, increasing the need for trauma-informed, survivor-focused support systems (Kumar & Gupta, 2021).
- Framework Viability:
  The suggested integrated framework, which includes changes to laws, strengthening institutions, AI monitoring, and digital literacy programs, offers a practical and scalable solution to address current gaps at both national and regional levels.

7. Recommendations

Based on the findings, the following multi-faceted policy actions are proposed:

- Legislative Reforms
  - ✓ Update the IT Act to include new cyber offenses like deepfake sharing, image morphing, and AI-based impersonation.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-2 | Issue-12 | December - 2024 | Page 104-117

- ✓ Sign the Budapest Convention, with suitable sovereignty protections, to support cross-border collaboration in cybercrime investigations.

- Institutional Reforms
  - ✓ Create a National Cybercrime Victim Support Agency to provide anonymous reporting, legal help, and counseling services.
  - ✓ Enhance cybercrime resources in Chhattisgarh, including creating specific cybercrime centers in rural and tribal areas for timely and local responses.
- Technological Innovations
  - ✓ Use AI detection systems for CSAM, deepfakes and image-based abuse, following the Personal Data Protection Act, 2019, and ethical AI guidelines.
- Awareness Initiatives
  - ✓ Start state-level campaigns and partner with NGOs to promote digital safety.
  - ✓ Aim for 50% female digital literacy in Chhattisgarh by 2025, with support from school programs, community outreach, and public education efforts.

8. Conclusion

India's rapid rise in cybercrime—from 21,796 cases in 2017 to 60,123 in 2022—shows not only the growing complexity of digital threats but also the shortcomings of current laws and institutions, particularly the IT Act and the POCSO Act, in tackling modern cyber risks. Regional differences, like those seen in Chhattisgarh with low digital literacy and weak cybercrime resources, further increase the vulnerability of women, children, and marginalized groups. This study suggests a framework focused on gender and children, based on updating laws, expanding institutions, using AI for monitoring, and grassroots awareness initiatives. Designed to be both scalable and adaptable, the model provides a feasible route to a safer and fairer digital environment. Looking ahead, future research should look into using blockchain technology to ensure secure reporting, data integrity, and chain-of-custody management in cybercrime investigations (Sharma, 2021). This could add an extra level of trust and transparency to digital justice systems.

References

1. Bose, A. (2021). Gender and cybercrime in India. "Indian Journal of Gender Studies", 28(3), 230–245. https://doi.org/10.1177/09715215211030590
2. hakraborty, S. (2020). Cybercrime and women in India: Issues and challenges. "Journal of Victimology and Victim Justice", 3(2), 150–165. https://doi.org/10.1177/2516606920965860
3. Ghosh, A., & Sinha, R. (2022). Regional disparities in cybercrime enforcement: A case study of Chhattisgarh. "Indian Journal of Criminology", 50(1), 25–40. https://ncrb.gov.in/sites/default/files/criminology_journal_2022.pdf
4. Jain, R. (2019). Cyber forensics in India: Challenges and prospects. "Journal of Indian Forensic Sciences", 41(3), 200–215. https://doi.org/10.1007/s41412-019-00234-5

5. Kumar, S., & Gupta, P. (2021). Cybercrime against women and children. "Indian Journal of Criminology", 49(2), 30–45. https://doi.org/10.1177/00195561211035308
6. Mishra, N. (2021). Social media and cybercrime: A study of platform governance in India. "Journal of Media Law and Ethics", 9(2), 80–95. https://doi.org/10.1177/17513072211001234
7. Patel, K. (2020). Cross-border cybercrime: India's legal limitations. "International Journal of Comparative Law", 8(3), 120–135. https://doi.org/10.1093/icon/mzaa012
8. Rao, S. (2022). AI applications in cybercrime prevention: Opportunities and risks. "Journal of Artificial Intelligence and Law", 5(1), 50–65. https://doi.org/10.1007/s40319-022-01145-3
9. Sharma, P. (2021). Global cybercrime strategies. "International Journal of Cybersecurity", 4(4), 100–115. https://doi.org/10.1093/cybsec/tyab012
10. Singh, M., & Sharma, A. (2021). Victim support systems in cybercrime: Lessons from global models. "Journal of Law and Social Policy", 14(2), 90–105. https://doi.org/10.1177/08258597211029789
11. Thomas, J. (2021). "Digital child protection in India" [Doctoral dissertation, Shodhganga@INFLIBNET]. http://shodhganga.inflibnet.ac.in/handle/10603/345678