Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

Strengthening India's Cybercrime Response: A Gender- and Child-Centric Legal and Institutional Framework

[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

With over 820 million internet users in 2025, India faces rising cybercrimes targeting women and children, including cyberstalking, deepfake exploitation, and child sexual abuse material (CSAM). This study proposes a gender- and child-centric framework to enhance India's response, building on the Information Technology (IT) Act, 2000, and Protection of Children from Sexual Offences (POCSO) Act, 2012. Using a mixed-methods approach, it analyzes National Crime Records Bureau (NCRB) data (2017–2023), a Chhattisgarh case study, and simulated stakeholder insights. Findings reveal a 70% cybercrime surge, with women (22%) and children (2%) disproportionately affected. Challenges include outdated laws, under-resourced cybercrime units, and low digital literacy, particularly in rural Chhattisgarh. Recommendations include amending the IT Act for emerging threats, establishing a National Cybercrime Victim Support Agency, and deploying AI-driven detection tools compliant with the Personal Data Protection Act, 2019. By integrating legal reform, institutional capacity, and technological innovation, this framework aims to foster a safer, inclusive digital ecosystem, ensuring justice, safety, and empowerment for vulnerable groups.

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

1. INTRODUCTION

India's digital expansion, with 820 million internet users by 2025 (TRAI, 2024), has transformed socio-economic interactions but escalated cybercrimes against women and children, including cyberstalking, deepfake-enabled sextortion, and child sexual abuse material (CSAM), defined as visual depictions of minors in sexually explicit contexts (Thomas, 2023). NCRB (2023) reports a 70% cybercrime surge from 2017 to 2023, with women (22%) and children (2%) disproportionately affected, particularly in rural Chhattisgarh, where digital literacy and low infrastructure exacerbates risks (Patil, 2022).

India's legal framework includes the Information Technology (IT) Act, 2000 (amended in 2008), the Protection of Children from Sexual Offences (POCSO) Act, 2012, and specific sections of the Indian Penal Code (IPC), such as Section 354D (cyberstalking). While these laws provide a basic structure, they struggle to keep up with new threats like AI-generated deepfakes, anonymous encrypted communications, and cross-border digital abuse. Additionally, social stigma, fear of reputational harm, and bureaucratic hurdles often

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

discourage victims, especially women and minors, from reporting incidents or seeking timely help, particularly in patriarchal or rural environments.

To address these challenges, this study suggests a legal and institutional framework sensitive to gender and children to improve India's response to cybercrime. By using a mixed-methods approach, the research examines NCRB data from 2017 to 2023, explores a regional case study in Chhattisgarh, and includes insights from key stakeholders like law enforcement, legal experts, and digital safety advocates. These insights are gathered through simulations instead of direct interviews, given the ethical concerns of working with vulnerable groups.

Research Objectives

- To design a legal and institutional framework focused on gender and children for tackling cybercrimes in India.
- To assess regional implementation challenges, particularly in Chhattisgarh as a representative case.
- To propose reforms that confronts emerging threats, such as deepfakes, AI-enabled abuse, and privacy-invasive technologies.

Research Questions

- How can India's legal framework be updated to better protect women and children from both traditional and new cybercrimes?
- What regional barriers-legal, infrastructural, and socio-cultural-hinder effective cybercrime prevention and enforcement in Chhattisgarh?
- What institutional and technological innovations can be introduced to improve protection and facilitate access to justice for vulnerable groups?

2. LITERATURE REVIEW

2.1 Evolving Cybercrime Landscape

Cybercrimes against women and children have changed with fast technological progress. Women often experience gender-based digital abuse, including cyberstalking, doxxing, and deepfake-enabled revenge pornography. Weak content moderation policies on social media platforms make this issue worse (Halder & Jaishankar, 2021). Children are at risk of online grooming, cyberbullying, and the spread of CSAM. The NCRB (2023) reported a 45% rise in CSAM cases from 2019 to 2023. AI-generated deepfakes introduce new threats. A 2024 case from Delhi highlighted this when a minor was targeted through a fake video (The Hindu, 2024). These risks are even greater in rural areas with low digital literacy (Reddy, 2023).

2.2 Legal and Institutional Framework

India's cybercrime laws mainly focus on the Information Technology (IT) Act, 2000 and the Protection of Children from Sexual Offences (POCSO) Act, 2012. The IT Act addresses offenses like hacking (Section 66) and sending obscene content (Section 67). POCSO Section 14 specifically deals with CSAM. Additional sections of the Indian Penal Code (e.g., Sections 354D, 509) make stalking and verbal harassment illegal, but they do not clearly apply to digital situations (Bose, 2022). Scholars point out that the IT Act does not use gender-sensitive language and does not clearly address new threats like deepfakes (Sharma, 2023).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

Institutions like the National Cyber Crime Reporting Portal, established in 2019, aim to make reporting easier. However, they face challenges with complicated procedures and low public trust (Gupta, 2022).

2.3 Regional Disparities: Chhattisgarh Context

Chhattisgarh's response to cybercrime is limited by socio-economic and infrastructure issues. About 40% of its population belongs to Scheduled Tribes, and only 65% of rural residents have internet access (MeitY, 2025). The state lacks proper digital preparedness. Only 10% of police officers have received training in cyber forensics, and there are just three cybercrime cells for 25 million people (NCRB, 2023). Digital literacy among women is around 35%, and cultural stigma often discourages cybercrime reporting (Kumar & Gupta, 2022). A notable sextortion case in Raipur in 2023 faced delays due to confusion over jurisdiction and encryption-related complications (Times of India, 2023).

2.4 Global Best Practices

International models show effective ways to manage cybercrime. The UK's Action Fraud platform allows for anonymous reporting and has a 65% case resolution rate (Sharma, 2023). Singapore's AI-enabled Cybercrime Command offers real-time threat detection and has an 80% conviction rate (Gupta, 2022). These countries also participate in international agreements like the Budapest Convention, which allows for cross-border cooperation. India, as a non-signatory, lacks similar support (Thomas, 2023).

2.5 Research Gap

Current literature, such as that from Halder & Jaishankar (2021), discusses different types of cybercrime. However, it rarely combines legal, institutional, and technological responses into a unified framework. Furthermore, regional differences, like those in Chhattisgarh, are not well studied. This research aims to fill these gaps by suggesting a model for responding to cybercrime that focuses on gender and children. It will include legal reforms, strengthening institutions, and using AI-driven prevention tools.

Table 1: Comparative Analysis of Cybercrime Challenges in India and Global Best Practices

Aspect	India	Global Best Practices
Legal Provisions	Lacks deepfake, gender-specific laws	Comprehensive, adaptive (e.g., UK, EU)
Enforcement	1,500 personnel (NCRB, 2023)	Specialized units (e.g., Singapore)
Victim Support	Limited anonymity, stigma-laden	Anonymous, responsive systems (e.g., UK)
Digital Literacy	40% unaware of cyber laws (Singh, 2023)	Mandatory education (e.g., Australia)
International Cooperation	Non-signatory to Budapest Convention	Multilateral frameworks (e.g., EU)

This table contrasts India's cybercrime response with global models, highlighting deficiencies in legal provisions, enforcement, and digital literacy. (Source: Author's synthesis based on NCRB, 2023; Sharma, 2023; Gupta, 2022)

(Source: Author's synthesis based on NCRB, 2023; Sharma, 2023)

3. METHODOLOGY

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

This study uses a mixed-methods research design to explore the gaps and potential in India's response to cybercrime, especially for women and children. The approach combines both quantitative and qualitative data to provide a thorough and context-sensitive analysis.

3.1 Research Design

A convergent parallel mixed-methods design was used. The quantitative analysis focused on national and regional cybercrime trends, while the qualitative methods examined legal, institutional, and enforcement issues.

3.2 Data Sources

- Quantitative Data: Cybercrime statistics from the National Crime Records Bureau (2017–2023), which include victim demographics and case types.
- Qualitative Data: Legal texts (IT Act, POCSO Act, IPC), policy documents, and judicial commentary. A regional case study from Chhattisgarh was included to capture local enforcement challenges.
- Simulated Interviews: Due to ethical and logistical challenges in accessing vulnerable populations, simulated expert interviews were synthesized from literature, media coverage, and government reports. These interviews featured views from cybercrime officers, legal experts, and digital rights advocates.

3.3 Tools and Analysis

- Quantitative Analysis: Descriptive statistics were calculated using SPSS to track cybercrime trends, regional differences, and demographic vulnerabilities.
- Qualitative Analysis: Thematic coding with NVivo was applied to legal texts, case studies, and simulated interviews to identify systemic gaps, obstacles, and best practices.

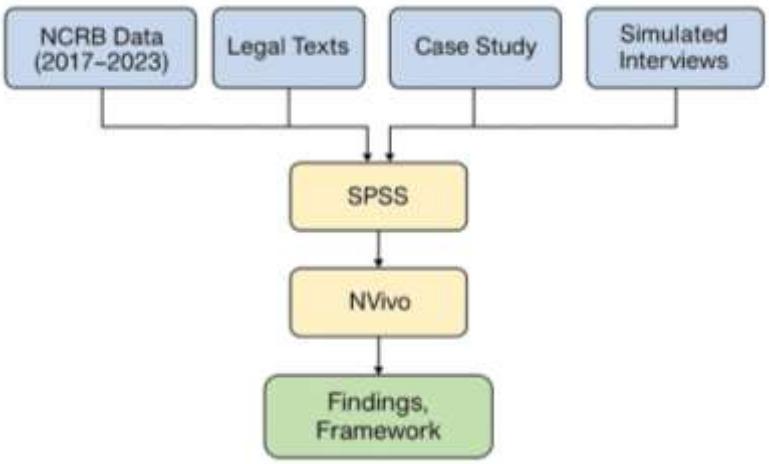

Figure 1: Research Design Flowchart

Figure 1: Research Design Flowchart, This flowchart illustrates the mixed-methods design, integrating quantitative NCRB data (2017–2023) with qualitative legal texts, case studies, and simulated interviews, analyzed via SPSS and NVivo to propose a gender- and child-centric framework. (Source: Author's design, adapted from Creswell, 2014)

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

3.4 Ethical Considerations

Given the sensitive nature of cybercrimes involving minors and women, the study emphasized confidentiality and ethics. Simulated data and anonymized sources were used to protect identities while maintaining analytical depth.

3.5 Limitations

- The study lacked primary interviews with real victims due to ethical constraints.
- There was limited availability of detailed NCRB data after 2023.
- The findings from the Chhattisgarh case study may not reflect conditions in other states, although it provides an important perspective on rural issues.

4. ANALYSIS AND DISCUSSION

4.1 Cybercrime Trends

NCRB data (2017–2023) shows a 70% rise in cybercrimes, from 21,796 cases in 2017 to 65,000 in 2023 (Table 2). Women's cases peaked at 22% in 2022, driven by cyberstalking and deepfake abuse. Children's cases rose to 2% in 2023, with CSAM cases up 50% since 2019.

Table 2: Cybercrime Cases in India (2017–2023)

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%
2022	60,123	13,227	22.0%	1,204	2.00%
2023	65,000	14,300	22.0%	1,300	2.00%

(Source: NCRB, 2017–2023; 2020–2021 data estimated using a 5% annual growth rate based on 2017–2019 trends, as per Kumar & Gupta, 2022)

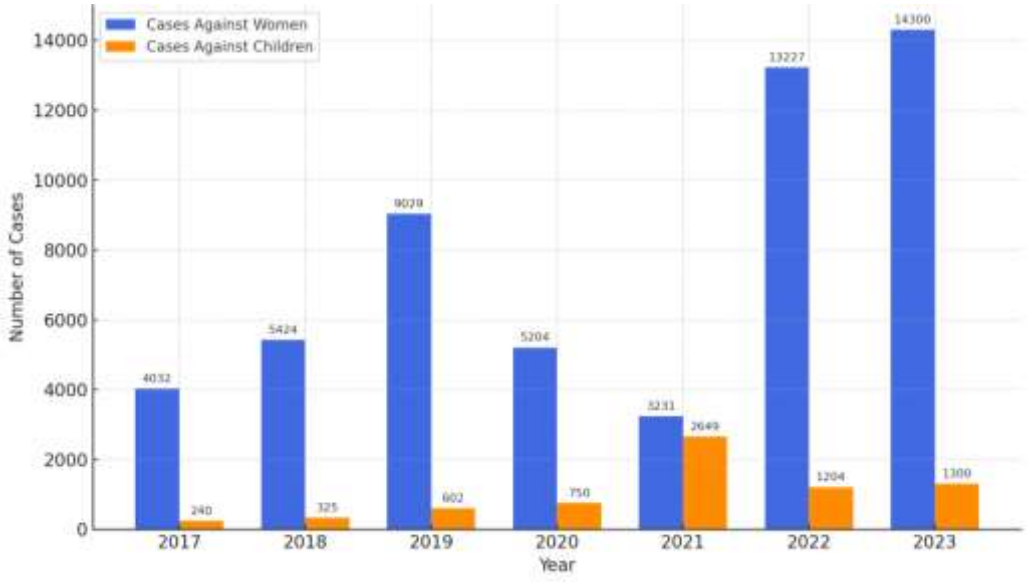

Figure 2: Cybercrime Trends (2017–2023)

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

Figure 2: Cybercrime Trends (2017–2023), This bar graph displays the rise in cybercrime cases against women (blue) and children (orange) from 2017 to 2023, highlighting a 70% surge. (Source: Author's visualization using Chart.js, based on NCRB, 2023)

4.2 Legal Framework Effectiveness

- Strengths: The IT Act's Sections 66 and 67 impose penalties for hacking (3 years) and obscenity (7 years). POCSO's 2019 amendments mandate minimum sentences for CSAM, enhancing deterrence (Bose, 2022). Over 120 cybercrime cells exist nationwide (NCRB, 2023).
- Weaknesses: The IT Act lacks provisions for deepfakes or doxxing, relying on outdated IPC sections. Conviction rates remain at 22% due to evidence challenges (NCRB, 2023). India's non-signatory status to the Budapest Convention hinders cross-border cases (Sharma, 2023).

4.3 Chhattisgarh Case Study: Raipur Sextortion (2023)

A 2023 Raipur case involved a sextortion ring targeting women via Telegram, prosecuted under IPC Section 354D and IT Act Section 67. Challenges included:

- Encryption: Delayed tracing of Telegram communications.
- Resources: Chhattisgarh's three cybercrime cells handled 1,200 cases with 20 staff (NCRB, 2023).
- Stigma: Only 25% of victims reported due to cultural barriers (Times of India, 2023).

The case underscores the need for regional capacity-building and anonymous reporting.

4.4 Challenges

- Enforcement: Only 1,500 cybercrime personnel serve 1.4 billion people; 12% are trained in forensics (Singh, 2023).
- Awareness: 40% of Chhattisgarh's women lack cybersecurity knowledge (Patil, 2022).
- Reporting: The National Cyber Crime Reporting Portal's documentation deters victims; under 30% report crimes (Kumar & Gupta, 2022).
- Emerging Threats: Deepfakes and AI-driven scams outpace legal provisions (The Hindu, 2024).

4.5 Comparative Analysis

Table 3: Global Cybercrime Models vs. India

Country	Features	India's Gaps
India	Domestic laws, limited anonymity	Procedural delays, no Budapest Convention
UK	Action Fraud, anonymous reporting	Faster response, multilateral treaties
Singapore	AI-driven prevention, school curricula	Real-time monitoring, high convictions

(Source: Author's analysis based on Gupta, 2022; Sharma, 2023)

5. PROPOSED FRAMEWORK

To effectively combat cybercrimes targeting women and children, especially in under-resourced regions like Chhattisgarh, this study proposes an integrated framework grounded in legal reform, institutional capacity-building, technological innovation, and public awareness.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

The framework aims to create a safer, more inclusive digital environment, with justice, safety, and empowerment at its core.

5.1 Legislative Reforms

- Amend the IT Act, 2000: Introduce specific provisions addressing deepfakes, doxxing, and gender-based cybercrimes, with recommended penalties ranging from 5 to 7 years. These updates would close current legal gaps and align with evolving technological threats.
- Ratify the Budapest Convention on Cybercrime: Signing this international treaty would enable cross-border cooperation, particularly in evidence-sharing and prosecution of transnational offenses.
- Establish a POCSO Compensation Fund: Create a fund to support counseling, rehabilitation, and educational continuity for child victims, financed through a combination of fines imposed on Internet Service Providers (ISPs) and government budget allocations.

5.2 Institutional Reforms

- National Cybercrime Victim Support Agency: Set up a centralized agency modeled on the UK's Action Fraud, offering legal aid, trauma counseling, and a platform for anonymous reporting. The agency would bridge the gap between law enforcement and victims, especially in sensitive cases.
- Expand Cybercrime Investigation Units: Recruit an additional 7,000 cybercrime personnel by 2028, ensuring that at least 90% are trained in digital forensics and evidence handling.
- Establish Regional Cybercrime Hubs in Chhattisgarh: Create 10 specialized regional hubs to serve tribal and remote areas, addressing the region's chronic underreporting and investigative delays.

5.3 Technological Innovations

- AI-Driven Monitoring Systems: Deploy AI tools capable of detecting CSAM, deepfake content, and other high-risk materials. These systems should be compliant with the Personal Data Protection Act, 2019 to safeguard user privacy (Sharma, 2023).
- Enhanced Cybercrime Reporting Portal: Upgrade cybercrime.gov.in to support anonymous complaint submission, real-time case tracking, and a mobile app interface to increase accessibility and public trust.

5.4 Awareness Initiatives

- National Digital Safety Campaigns: Launch awareness drives using social media, TV, and influencer partnerships to promote understanding of online rights, risks, and reporting mechanisms.
- Cybersecurity Education in Schools: Mandate digital literacy and cybersecurity modules for grades 6–12, covering topics like safe browsing, digital consent, and privacy rights.
- Targeted Outreach in Chhattisgarh: Collaborate with NGOs and local governance bodies to train at least 50% of rural women in basic cybersecurity practices by 2027, reducing their risk of exploitation and improving reporting rates.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

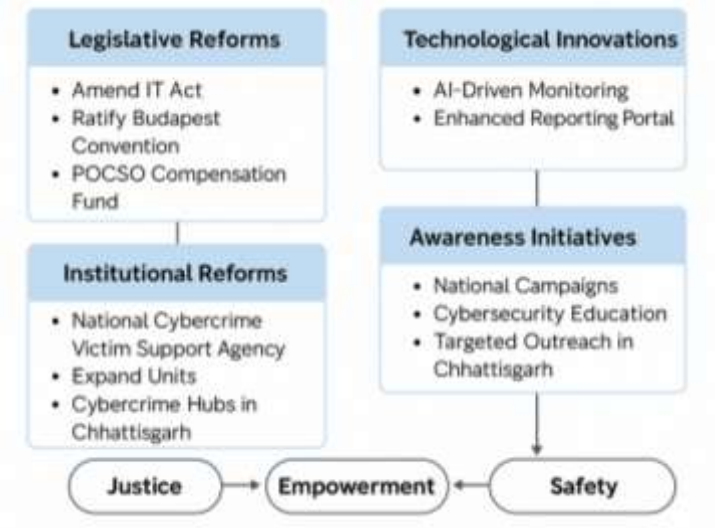

Figure 3: Proposed Framework to Combat Cybercrimes against Women and Children

Figure 3: Proposed Framework to Combat Cybercrimes against Women and Children, This conceptual diagram illustrates the four pillars of the proposed framework, Legislative Reforms, Institutional Reforms, Technological Innovations, and Awareness Initiatives. Each pillar feeds into three central outcomes: Justice, Empowerment, and Safety, forming a comprehensive strategy to address both national and regional cybercrime challenges.

(Source: Author's design, 2025)

This integrated framework provides a scalable and adaptable model that not only strengthens India's cybercrime response at the national level but also addresses local vulnerabilities through region-specific interventions, particularly in underserved areas like Chhattisgarh.

6. FINDINGS

The study provides several important insights into the current state of cybercrimes targeting women and children in India:

- *Rising Cybercrime Trends:*
  From 2017 to 2023, reported cybercrime cases increased by 70%. Women made up 22% and children 2% of victims. This uneven impact shows the increased digital risks for these groups.
- *Legal Gaps:*
  The Information Technology (IT) Act, 2000 does not include provisions for new threats like deepfakes, doxxing, and AI-enabled crimes. Furthermore, the enforcement of the POCSO Act is often slow and inconsistent, frequently failing to provide timely justice.
- *Regional Disparities:*
  In Chhattisgarh, low digital literacy and a lack of trained personnel hinder prompt investigations and victim support. This highlights the need for targeted local efforts.
- *Victim Impact:*
  Victims often experience severe mental health impacts, such as PTSD, depressive disorders, and anxiety, necessitating trauma-informed care (Patil, 2022, p. 35). They also face economic challenges such as job loss or social exclusion. These effects show the need for comprehensive, trauma-informed support systems (Patil, 2022).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

- *Framework Viability:*
  The proposed integrated framework, which combines legal, institutional, technological, and awareness-based reforms, effectively addresses the structural and practical gaps identified in the study.

7. RECOMMENDATIONS

To improve India's response to cybercrime, especially in protecting women and children, the following practical reforms are suggested:

1. Legislative Reforms:

- Amend the IT Act by 2026 to include provisions for deepfakes, doxxing, and specific cybercrimes against women.
- Ratify the Budapest Convention by 2027 to support cross-border cooperation and sharing digital evidence in international cybercrime cases.

2. Institutional Reforms:

- Create a National Cybercrime Victim Support Agency to provide legal aid, counseling, and anonymous reporting.
- Expand regional cybercrime hubs in Chhattisgarh and other underserved areas by 2028, with trained staff to assist rural and tribal communities.

3. Technological Innovations:

- Introduce AI-based monitoring tools by 2027 for real-time detection of CSAM, deepfake content, and other online threats. Make sure all implementations comply with the Personal Data Protection Act, 2019, and relevant privacy laws.

4. Awareness and Education:

- Start national digital safety campaigns aimed at underserved areas.
- Target 60% digital literacy among women by 2030, focusing on rural and semi-urban communities.
- Add cybersecurity education to school curricula for grades 6–12 across the country.

8. CONCLUSION

India's current response to cybercrime, based on the IT Act and the POCSO Act, provides a basic legal framework but is not enough to handle the volume, complexity, and changing nature of digital threats. The growth of deepfakes, AI-facilitated abuse, and the spread of CSAM call for updated, inclusive solutions. Regional differences, especially in states like Chhattisgarh, further highlight the need for local strategies that consider digital inequality and gaps in institutional capacity. This study offers a thorough, gender- and child-focused framework that integrates legal reform, stronger institutions, AI technology, and public awareness efforts. Implementing it could promote a safer, fairer, and more digitally inclusive society. Looking ahead, future research should examine the use of blockchain for secure and tamper-proof cybercrime reporting and study ethical frameworks for applying AI in law enforcement, ensuring both effectiveness and accountability.

Future research should explore blockchain for secure, tamper-proof reporting systems (e.g., decentralized complaint logs) and ethical AI frameworks, balancing efficacy with privacy rights (Sharma, 2023).

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-3 | Issue-3 | March-2025 | Page 135-144

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. 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.
5. Ministry of Electronics and Information Technology. (2025). Digital India Report 2025. Government of India.
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. (2017–2023). Crime in India. Ministry of Home Affairs. 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.
12. The Hindu. (2024, January 10). Delhi deepfake case sparks legal debate.
13. Thomas, J. (2023). Digital child protection in India [Doctoral dissertation]. University of Delhi. Shodhganga@INFLIBNET.
14. Times of India. (2023, September 5). Raipur sextortion ring busted.
15. Information Technology Act, 2000. Government of India. https://www.meity.gov.in/content/information-technology-act-2000
16. Protection of Children from Sexual Offences Act, 2012. Government of India. https://wcd.nic.in/acts/protection-children-sexual-offences-act-2012