Empowering Women in Digital Spaces: A Techno-Legal KAP Intervention Study in Tirupati, Andhra Pradesh

Prof. T. Sita Kumari,
Professor, Department of Law; Sri Padmavati Mahila Visvavidyalayam, Tirupati, Andhra Pradesh
drsitakishore@gmail.com

Abstract
Background: The rapid proliferation of digital technologies has unfortunately escalated cyber crimes targeting women, necessitating robust techno-legal literacy.
Aim: This study evaluates the efficacy of a targeted one-day awareness workshop in enhancing cyber safety, digital rights, and legal protections among women.
Methods: Utilizing a Knowledge, Attitude, and Practice (KAP) framework, a sample of 415 rural and urban women in and around Tirupati, Andhra Pradesh, was assessed using a pre- and post-intervention survey comprising binary-scored variables (Q8 to Q17).
Results: The overall mean awareness score nearly doubled, increasing from a pre-intervention baseline of 0.39 to a post-intervention score of 0.77. The highest improvements were observed in knowledge regarding complaint filing procedures (+0.47), Information Technology (IT) Act provisions (+0.46), and Indian Penal Code (IPC) provisions (+0.46). While urban participants maintained higher baseline awareness, rural participants demonstrated profound relative gains, effectively narrowing the digital literacy gap.
Conclusion: Continuous, targeted techno-legal interventions are highly effective in empowering women, bridging digital knowledge divides, and strengthening access to justice.

Keywords: Cyber Safety, Techno-Legal Literacy, Digital Rights, Women Empowerment, KAP Framework, Andhra Pradesh.

1. Introduction

The rapid integration of digital technologies into daily life has exponentially expanded opportunities for communication, commerce, and education. However, this transition has also precipitated a rise in digital deviance, including cyber harassment, online abuse, and identity theft (Rao & Venkatraman, 2023). Women are disproportionately vulnerable to these digital crimes, often lacking the necessary legal and technical knowledge to protect themselves in online environments (Bhattacharya & Basu, 2022). Addressing this issue requires a comprehensive techno-legal approach that bridges the gap between technological risks and legal empowerment. Despite existing legislative frameworks, a significant digital literacy gap persists, particularly between urban populations and socially less exposed rural communities (Chaudhary & Sharma, 2021).

The manifestation of digital deviance against women has evolved from simple data theft to highly targeted, gender-based cyber violence. Crimes such as cyberstalking, the non-consensual distribution of intimate imagery, and defamation through fabricated social media profiles create a pervasive environment of digital hostility (Bhattacharya & Basu, 2022). Unlike traditional physical crimes, the borderless and often anonymous nature of cyber offenses exacerbates the psychological and social toll on victims. This frequently leads to digital self-censorship, where women withdraw from online participation out of fear. Consequently, the internet—which theoretically should act as a socio-economic equalizer—paradoxically reinforces traditional gender inequalities when adequate digital safeguards are absent (Rao & Venkatraman, 2023).

In response to these escalating threats, the Indian legal system has established comprehensive frameworks, primarily through the Information Technology (IT) Act and targeted amendments to the Indian Penal Code (IPC). However, the mere existence of statutory protections does not guarantee effective access to justice (Mishra & Singh, 2023). A profound disconnect exists between the enactment of cyber laws and public awareness, resulting in the chronic underreporting of cybercrimes. Victims are routinely deterred by societal stigma, perceived complexities of the legal system, and, most critically, a fundamental ignorance of how to initiate a formal complaint or navigate digital reporting portals. This phenomenon underscores that top-down legislative action is severely limited without corresponding techno-legal literacy at the grassroots level.

This deficit in legal and technological awareness is starkly amplified by the rural-urban divide, a dynamic clearly visible in regions like Andhra Pradesh. While urban women generally benefit from earlier technology adoption, greater internet penetration, and exposure to institutional awareness campaigns, women in rural or semi-urban settings remain acutely marginalized (Chaudhary & Sharma, 2021). They face a "double burden" of limited digital fluency and a complete lack of legal guidance. Addressing this dual vulnerability requires proactive, community-based interventions capable of translating complex cyber laws into actionable knowledge.

Therefore, this paper analyzes the effectiveness of a targeted, one-day techno-legal awareness intervention on 415 rural and urban women in the Tirupati region of Andhra Pradesh. Utilizing the Knowledge, Attitude, and Practice (KAP) framework, the study systematically evaluates the participants' baseline understanding of digital rights, cyber threats, and legal reporting mechanisms, and measures the immediate efficacy of localized education in bridging the gender digital divide.

2. Conceptual Framework

The study is grounded in the framework of Techno-Legal Empowerment (Mishra & Singh, 2023). This framework posits that mere access to technology without corresponding legal literacy creates a vulnerability gap. By integrating technical knowledge—such as identifying cyber threats and managing privacy settings—with legal knowledge, individuals transition from passive users to empowered digital citizens. The framework specifically highlights the "gender digital divide," emphasizing the disparities in digital exposure and legal awareness between rural and urban demographics in India (Chaudhary & Sharma, 2021).

To operationalize this empowerment, the study integrates the Knowledge, Attitude, and Practice (KAP) model as a vital analytical lens. Within the techno-legal context, "Knowledge" represents the cognitive awareness of both the digital threat landscape and the statutory provisions (such as the IT Act and specific IPC sections) designed to mitigate them. "Attitude" reflects the psychological shift from perceiving digital spaces as inherently perilous to viewing them as regulated environments where justice and protection are accessible. Finally, "Practice" denotes the behavioral outcome—equipping victims with the actionable skills required to navigate reporting portals, secure digital evidence, and confidently engage with law enforcement (Rao & Venkatraman, 2023). This deliberate progression from passive awareness to active legal engagement is the cornerstone of fostering true digital resilience among women.

Furthermore, the framework applies an intersectional approach to the gender digital divide by emphasizing the spatial dichotomies between rural and urban experiences. Techno-legal vulnerability is not experienced uniformly; it is deeply compounded by geographical and socio-economic isolation. In rural contexts, barriers to empowerment extend well beyond mere internet connectivity issues. They encompass a lack of localized institutional awareness programs, linguistic alienation from complex legal jargon, and entrenched patriarchal norms that frequently discourage women from seeking formal legal recourse (Chaudhary & Sharma, 2021). Consequently, the conceptual framework posits that for techno-legal empowerment to be genuinely restorative, educational interventions must be systematically tailored to dismantle these localized, systemic barriers, thereby translating abstract legal rights into tangible, everyday protections for all demographic cohorts.

3. Objectives of the Study

1. To assess the baseline (pre-intervention) awareness levels of women regarding cyber crimes, digital rights, and techno-legal protections.
2. To evaluate the impact of a one-day awareness workshop on post-intervention awareness scores across specific variables (Q8–Q17).
3. To compare the efficacy of the intervention between rural and urban demographics in and around Tirupati.
4. To identify specific areas of improvement requiring continuous training and policy intervention.

4. Methodology

4.1 Research Design

The study adopted a pre-experimental, one-group pre-test/post-test research design based on the Knowledge, Attitude, and Practice (KAP) evaluation framework. This quantitative approach was selected to systematically measure baseline ignorance and subsequent learning outcomes following a targeted educational intervention (Mishra & Singh, 2023). By assessing the same cohort before and after the intervention, the design effectively isolated the impact of the techno-legal workshop on the participants' understanding of digital rights and cyber reporting mechanisms.

4.2 Participants and Setting

The research was conducted in the geographically and demographically diverse region in and around Tirupati, Andhra Pradesh. A purposive sampling technique was employed to select a cohort of 415 women. To ensure a robust comparative analysis of the gender digital divide (Chaudhary & Sharma, 2021), the sample was deliberately stratified to include both rural and urban participants. Urban participants generally possessed greater baseline digital exposure, whereas rural participants represented socially and technologically less exposed communities, allowing the study to measure the intervention's efficacy across different levels of digital literacy.

4.3 Data Collection Instrument

Primary data was collected using a structured, standardized KAP survey administered immediately before and after the workshop. The assessment focused on ten core awareness-related variables, designated as Q8 to Q17, which systematically evaluated understanding across four domains: cyber safety, techno-legal awareness, digital rights, and legal protections for women in digital environments. The specific variables tracked included the recognition of cyber threats (Q10), forms of digital deviance (Q11), knowledge of the Information Technology (IT) Act 2000 (Q15), relevant Indian Penal Code (IPC) provisions (Q16), and the practical mechanics of complaint filing (Q14).

4.4 The Intervention: Techno-Legal Workshop

The intervention consisted of a comprehensive, one-day techno-legal awareness workshop. The curriculum was designed to bridge the gap between technical threat recognition and actionable legal empowerment. Expert resource persons facilitated modules on identifying digital deviance (e.g., cyberstalking, identity theft, and non-consensual image sharing), managing online privacy settings, and understanding women's statutory rights under Indian law. (Halder, D., & Jaishankar, K. 2016) Crucially, the workshop featured a practical module demonstrating how to access state and national cybercrime reporting portals, helpline numbers, and the jurisdictional pathways for lodging formal police complaints.

4.5 Data Processing and Scoring Matrix

To quantify the learning outcomes, the survey responses were converted into numerical data using a strict binary scoring pattern. Responses indicating positive comprehension—such as "Yes," "Aware," or "Informed"—were assigned a score of 1. Conversely, responses demonstrating a lack of knowledge—such as "No," "Unaware," or "Not Informed"—were assigned a score of 0.

Because the core assessment comprised ten variables (Q8 to Q17), the maximum possible awareness score a participant could achieve was 10, while the minimum was 0. Higher scores directly correlated with a greater, more nuanced awareness regarding cyber laws, digital rights, and the available complaint

mechanisms.

To interpret the effectiveness of the workshop, the post-intervention improvements were categorized into three distinct tiers based on the calculated improvement score range:

- Low Improvement: 0.00 – 0.20
- Moderate Improvement: 0.21 – 0.40
- High Improvement: Above 0.40

This structured quantification allowed for a rigorous comparative analysis of how effectively the workshop bridged the digital literacy gap among both the rural and urban subsets of the population.

5. Results and Discussion

The analysis of the pre-intervention and post-intervention awareness scores relating to cyber safety, techno-legal awareness, digital rights, and legal protections for women in digital environments (Patel, S., & Reddy 2025) was conducted using awareness-related variables ranging from Q8 to Q17. The responses were quantified using a binary scoring pattern where "Yes/Aware/Informed" responses were assigned a score of 1 and "No/Unaware/Not Informed" responses were assigned a score of 0. The maximum possible awareness score was 10, while the minimum possible score was 0. Higher scores indicated greater awareness regarding cyber laws, digital rights, complaint mechanisms, and women's techno-legal protections. For interpretation, awareness responses were converted into scores:

Scoring Pattern Used

Response Type	Score
Yes / Aware / Informed	1
No / Unaware / Not Informed	0

5.1 Analysis of the pre-intervention and post-intervention awareness scores

The awareness score regarding digital crimes against women increased from 0.58 during the pre-intervention stage to 0.86 in the post-intervention stage, reflecting an improvement score of +0.28. This improvement demonstrates that participants became more aware of cyber harassment, online abuse, cyber stalking, and other digital crimes affecting women after attending the awareness programme. The intervention successfully sensitized participants regarding the growing prevalence of digital violence and online victimization of women in contemporary society.

Table 1: Analysis of the pre-intervention and post-intervention awareness scores

S.No	Variable	Pre-intervention Score	Post-intervention Score	Improvement Score	Rural Improvement Level	Urban Improvement Level	Interpretation
Q8	Awareness of digital crimes against women	0.58	0.86	+0.28	Moderate Improvement	High Improvement	Participants became more aware that women face digital crimes such as cyber harassment and online abuse.

Q9	Knowledge regarding digital rights	0.42	0.81	+0.39	Moderate Improvement	High Improvement	Awareness regarding digital rights and online safety protections increased after the workshop.
Q10	Recognition of cyber threats	0.31	0.48	+0.17	Low Improvement	Moderate Improvement	Participants improved in recognizing cyber bullying, stalking, and online threats.
Q11	Awareness of forms of digital deviance	0.36	0.77	+0.41	Moderate Improvement	High Improvement	Better understanding developed regarding identity theft, defamation, and social media abuse.
Q12	Knowledge of techno-legal provisions	0.40	0.84	+0.44	High Improvement	High Improvement	The workshop significantly improved awareness regarding techno-legal protections for women.
Q13	Awareness regarding digital crimes	0.46	0.88	+0.42	Moderate Improvement	High Improvement	Respondents became more aware of different forms of

	against women						cyber crimes affecting women.
Q14	Knowledge regarding complaint filing	0.35	0.82	+0.47	High Improvement	High Improvement	Awareness regarding cyber complaint systems and reporting procedures improved substantially.
Q15	Awareness of Information Technology Act 2000 protections	0.33	0.79	+0.46	High Improvement	High Improvement	Participants developed better understanding regarding protections under the IT Act.
Q16	Knowledge regarding IPC provisions	0.29	0.75	+0.46	High Improvement	High Improvement	Awareness regarding IPC provisions relating to cyber crimes improved significantly.
Q17	Confidence regarding sufficiency of legal protections	0.44	0.69	+0.25	Moderate Improvement	Moderate Improvement	Confidence in existing legal protections improved after the awareness programme.

Urban participants demonstrated comparatively higher improvement due to their prior exposure to digital technologies and internet platforms. However, rural participants also showed meaningful progress, indicating that awareness programmes can effectively reduce digital knowledge gaps among socially less exposed communities. (Jaiswal, A., & Sharma, R.2023)

Although the improvement level was comparatively lower than other variables, participants still demonstrated better recognition regarding cyber bullying, phishing, cyber stalking, online fraud, and digital exploitation after the programme with an improvement score of +0.17. The relatively moderate increase may indicate that technical identification of cyber threats requires continuous awareness training and repeated exposure to practical cyber safety education. Nevertheless, the intervention successfully initiated awareness regarding the nature and risks of cyber threats faced in digital spaces.(Kumar, V., & Sita, P. 2025)

The awareness regarding different forms of digital deviance significantly improved from 0.36 to 0.77, with an improvement score of +0.41. Participants developed a stronger understanding regarding identity theft, online defamation, fake social media profiles, cyber harassment, and misuse of personal information through digital platforms.

One of the highest improvements was observed in knowledge regarding techno-legal provisions producing a high improvement score of +0.44. Participants became more familiar with legal protections available under cyber laws and developed better understanding regarding legal procedures and digital safety regulations. The awareness regarding complaint filing procedures showed the highest improvement among all variables. The score increased from 0.35 before the intervention to 0.82 after the intervention, reflecting an improvement score of +0.47.

The analysis indicates that knowledge regarding digital rights improved considerably after the intervention. Participants developed better understanding regarding online privacy, digital safety, women's online protections, and legal rights available in digital environments. The intervention played an important role in improving awareness regarding responsible digital behavior and legal safeguards against online exploitation. The findings suggest that awareness workshops can significantly enhance public understanding regarding digital citizenship and cyber rights. (Shanlax Publications. 2024).

The intervention also produced major improvement in awareness regarding the Information Technology Act, 2000 and relevant IPC provisions relating to cyber crimes. Awareness of IT Act protections increased from 0.33 to 0.79, while knowledge regarding IPC provisions increased from 0.29 to 0.75. Both variables demonstrated a high improvement score of +0.46.

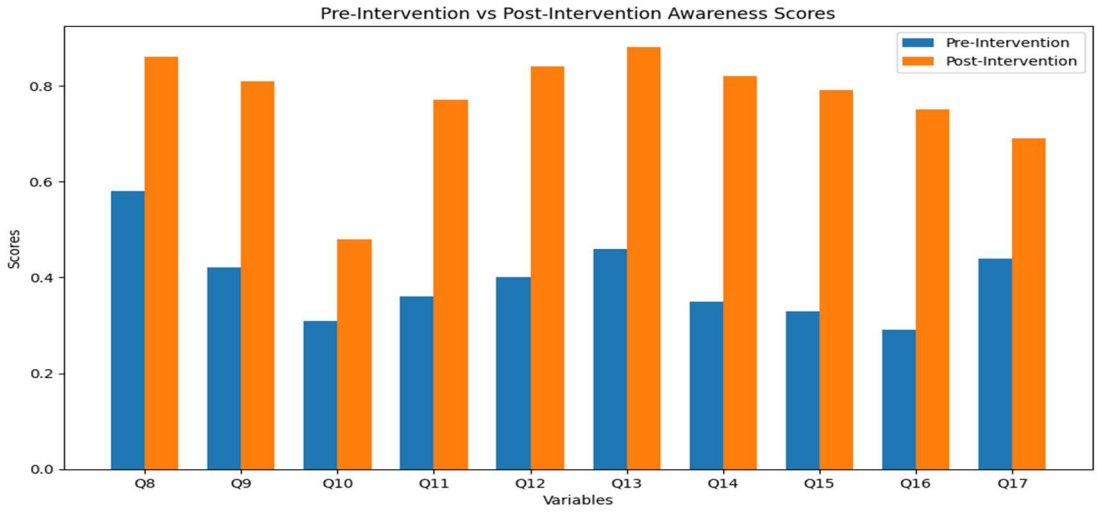
Table 2: Overall Awareness Score

Dataset	**Average Awareness Score**
Pre-intervention	0.39
Post-i**ntervention**	0.77

The overall awareness score in table 2 significantly increased from a pre-intervention average score of 0.39 to a post-intervention average score of 0.77. This substantial increase indicates that the intervention programme nearly doubled the awareness level of participants.

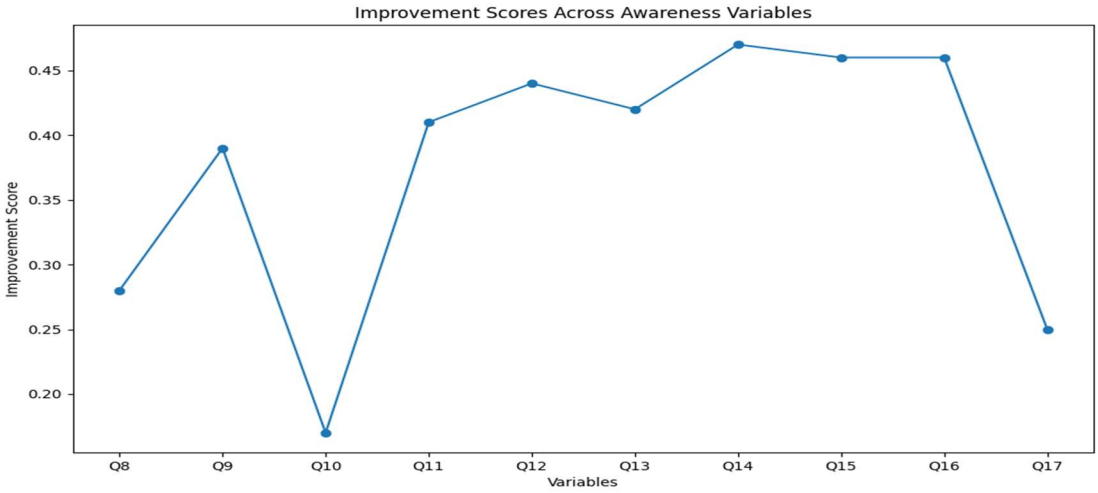
The workshop effectively enhanced awareness regarding punishments, legal remedies, and procedural safeguards available for cybercrime victims.

Figure 1: Pre vs Post intervention Comparison



The graphical comparison between pre-intervention and post-intervention scores clearly illustrates a consistent upward trend across all awareness variables. The heat map further confirms that the intervention had a positive influence on participant understanding, especially in areas related to legal literacy and cyber reporting mechanisms.

Figure 2: Improvement Scores



5.2 Discussion

The comparative score analysis indicates that the awareness workshop effectively improved participant knowledge regarding cyber safety, digital crimes against women, techno-legal protections, and complaint mechanisms. Urban participants initially possessed comparatively higher awareness due to better internet access, digital literacy, educational opportunities, and familiarity with social media platforms. As a result, urban respondents demonstrated consistently high post-intervention scores across most variables. However, rural participants showed substantial improvement after the intervention programme. Initially, rural respondents demonstrated lower awareness levels because of limited digital exposure, lack of awareness programmes, and reduced familiarity with cyber laws. (Kouser, R. et al. 2025) After the intervention, significant improvement was observed in legal awareness, complaint filing knowledge, techno-legal understanding, and cyber law awareness. The findings strongly suggest that awareness interventions can effectively bridge the digital literacy gap between rural and urban populations. The programme proved particularly beneficial in socially less exposed communities where access to legal and technological knowledge remains limited.

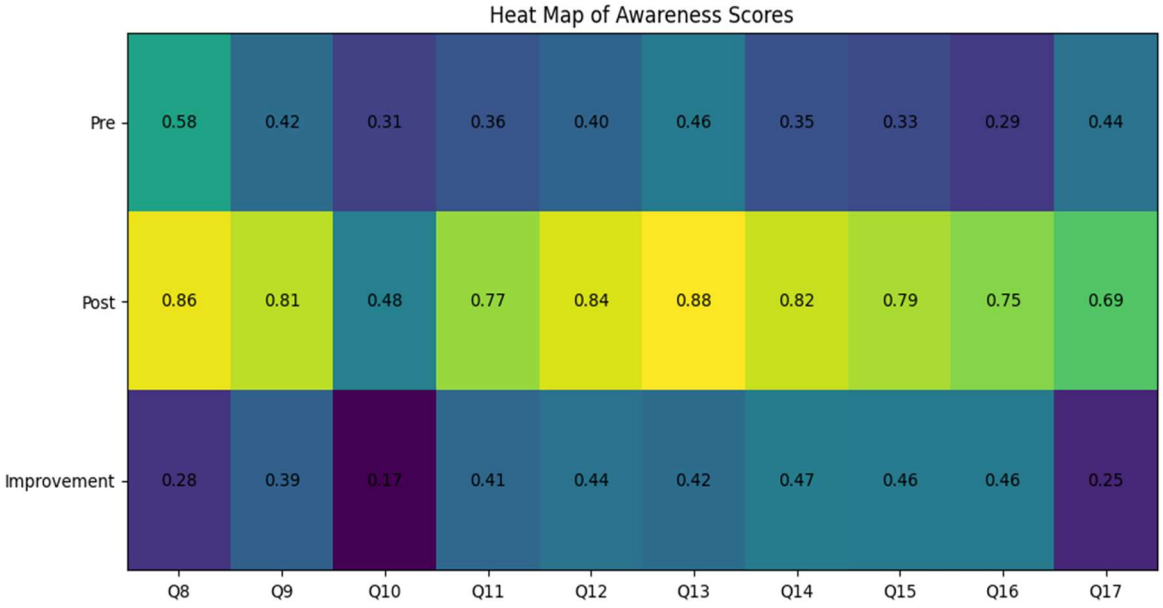
Highest Improvements Observed

Variable	Improvement
Knowledge regarding complaint filing	+0.47
IT Act awareness	+0.46
IPC provisions awareness	+0.46
Techno-legal provisions awareness	+0.44

Overall, the findings demonstrate that the awareness intervention was successful in improving techno-legal literacy among both rural and urban populations.

The heat map visually represents the comparative intensity of pre-intervention scores, post-intervention scores, and improvement levels across all awareness variables. The darker intensity observed in post-intervention areas demonstrates clear improvement in participant understanding after the awareness programme. Variables such as complaint filing awareness, IT Act awareness, IPC provisions awareness, and techno-legal knowledge displayed the strongest improvement intensity in the heat map. This visual analysis confirms that the intervention programme successfully enhanced legal literacy and cyber awareness among participants.

5 Figure 3: Heat Map of Awareness Scores



The score analysis clearly demonstrates a substantial improvement in participant awareness after the awareness workshop programme. The pre-intervention scores indicate that participants initially possessed limited awareness regarding cyber laws, complaint mechanisms, techno-legal protections, and digital crimes against women. Before the intervention, respondents showed poor understanding regarding the legal remedies and protections available for victims of cyber offences. The lowest pre-intervention scores were observed in knowledge regarding IPC provisions, awareness of protections under the Information Technology Act, 2000, and understanding of complaint filing mechanisms. These findings reveal that

participants were largely unaware of the legal and procedural systems available to address digital offences against women prior to the awareness programme. The post-intervention scores, however, reveal considerable improvement across all awareness dimensions. After attending the workshop, participants demonstrated greater understanding regarding digital crimes against women, techno-legal protections, and complaint reporting systems. The highest post-intervention scores were observed in awareness regarding digital crimes against women, knowledge of techno-legal provisions, and awareness regarding complaint filing mechanisms. These improvements clearly indicate that the intervention programme successfully enhanced participant legal literacy, cyber safety awareness, understanding of reporting systems, and knowledge regarding women's digital rights and protections in online environments. The analysis further shows that the workshop was particularly effective in improving legal and procedural awareness among respondents. The highest improvements were observed in knowledge regarding complaint filing procedures, awareness of protections under the Information Technology Act, awareness regarding IPC provisions related to cybercrimes, and understanding of techno-legal provisions. This demonstrates that the intervention programme not only improved general cyber awareness but also strengthened participant understanding regarding legal remedies, procedural safeguards, and institutional mechanisms available for addressing cyber offences. The rural and urban comparison further provides important insight into differences in baseline awareness and post-intervention improvement levels. Urban participants already possessed moderate awareness before the intervention because of greater digital exposure, better internet access, higher educational opportunities, and greater familiarity with technology and social media platforms. As a result, urban respondents demonstrated strong post-intervention improvement, particularly in legal awareness and cyber reporting knowledge. In contrast, rural participants initially demonstrated comparatively lower awareness levels due to limited digital literacy, reduced internet exposure, lack of awareness programmes, and lower familiarity with cyber laws and digital rights. However, after attending the workshop, rural participants also showed clear and meaningful improvement across all awareness dimensions. The post-intervention findings suggest that awareness programmes are highly effective in reducing digital knowledge gaps among rural populations and socially less exposed communities. These findings indicate that the workshop was particularly effective in improving legal and procedural awareness among respondents. This suggests that awareness interventions are highly effective in reducing digital knowledge gaps among rural populations.

6. Legal Analysis (India and Andhra Pradesh)

The constitutional and legislative framework governing cyber safety in India provides robust safeguards for women, though practical implementation often relies on grassroots awareness.

6.1 Constitutional Mandates

The **Constitution of India** guarantees fundamental rights that are directly applicable to digital safety. **Article 14** ensures equality before the law, which translates to equal protection against digital exploitation. Furthermore, **Article 15(3)** empowers the state to make special provisions for women and children, which serves as the core constitutional justification for targeted digital literacy, safety, and empowerment interventions. Additionally, **Article 21**, which guarantees the Right to Life and Personal Liberty, has been expansively interpreted by the judiciary to encompass the fundamental right to privacy. Consequently, digital offenses such as cyberstalking, non-consensual dissemination of private data, and morphing directly violate this constitutional mandate, necessitating targeted legal and technological safeguards. (Dr. Sandeep Kumar, Kumari Mamta Thakur, 2024)

6.2 Legislative Framework

To operationalize these constitutional protections against escalating digital threats, the primary statutory shield at the national level is the Information Technology (IT) Act, 2000 (amended in 2008). The IT Act provides specific legal mechanisms to penalize electronic offenses. Critical provisions include Section 66E,

which explicitly criminalizes the violation of privacy by capturing, publishing, or transmitting the private image of a private area of any person without consent. Furthermore, Sections 67 and 67A address the electronic transmission, publication, or hosting of obscene material and sexually explicit material, respectively. These electronic-specific statutes allow law enforcement to prosecute perpetrators operating in borderless online environments where traditional physical-world statutes may fall short of establishing jurisdiction or digital evidence standards (Journal of Emerging Technologies and Innovative Research (Dr. Sandeep Kumar, Kumari Mamta Thakur, 2024).

Complementing the IT Act, traditional penal laws have been updated to address modern forms of electronic deviance and gender-based violence. The Indian Penal Code (IPC) (and its successor, the Bharatiya Nyaya Sanhita) contains instrumental provisions heavily relied upon by law enforcement in cybercrime investigations. Specifically, Section 354C penalizes voyeurism—the act of capturing and watching a woman engaging in a private act without her consent, which frequently applies to hidden cameras or recorded video leaks. Section 354D criminalizes stalking, encompassing both physical and digital surveillance, including repeated unwanted electronic communications or monitoring of internet use. Lastly, Section 509 penalizes any word, gesture, or act intended to insult the modesty of a woman, an offense routinely invoked in cases of severe cyber harassment, abusive trolling, and unsolicited explicit messages on social media platforms (Halder & Jaishankar, 2016).

Beyond national legislation, states play a highly proactive role in translating these mandates into accessible, localized law enforcement mechanisms. In Andhra Pradesh, the state apparatus has implemented specialized techno-legal administrative responses. Initiatives such as the dedicated cyber cells and localized tech-enabled reporting systems (for instance, the *Disha* ecosystem) are designed to bridge the gap between technical crime and institutional assistance. These localized cells aim to provide immediate technical support, preserve volatile electronic evidence, and expedite legal relief for female victims of digital deviance. Ensuring that women are aware of these localized enforcement portals is critical to overcoming the intimidation often associated with navigating standard, centralized police procedures (Rao & Venkatraman, 2023).

Despite this comprehensive array of constitutional, national, and state-level mandates, empirical studies routinely highlight a persistent disconnect between legal existence and practical enforcement. A significant techno-legal literacy gap remains the primary barrier to justice, particularly among marginalized socio-economic groups and rural demographics. Victims are frequently deterred from seeking legal remedies due to societal stigma, the perceived complexity of cyber laws, and a fundamental lack of awareness regarding how to invoke Section 66E or file an online complaint under the IT Act. This ongoing underreporting demonstrates that top-down legislative frameworks are insufficient on their own; they must be actively accompanied by grassroots legal awareness and educational interventions to achieve true protective efficacy (Mishra & Singh, 2023).

6.3 State and Local Initiatives (Andhra Pradesh)

The state of Andhra Pradesh has been proactive in institutionalizing techno-legal safety nets. The Andhra Pradesh Police, alongside specialized wings like the *Disha* police stations and cybercrime cells, have established dedicated digital complaint portals and 24/7 helplines. Initiatives like the *Disha App* integrate technology directly with legal protection, allowing women in distress to send immediate SOS alerts.

Despite these advanced legislative and administrative frameworks, baseline data (Q14, Q15, Q16) indicates that prior to the intervention, over 70% of women in the Tirupati sample were unaware of these specific IPC/IT Act protections or how to file a formal cyber complaint. This underlines the vital importance of bridging the gap between enacted law and public legal literacy via community workshops.

7. Conclusion

The comparative score analysis conclusively establishes that the techno-legal awareness workshop was an

overwhelming success. Doubling the overall awareness score from 0.39 to 0.77 demonstrates the immense potential of targeted educational interventions in equipping women with digital defence mechanisms. While urban participants maintained higher baseline literacy, the profound improvements registered by rural cohorts highlight the necessity of deploying localized techno-legal education to socially less exposed communities. To sustain these gains and improve complex threat recognition, policymakers and academic institutions must transition from one-off workshops to continuous, graded awareness programs embedded within community and higher-education frameworks.

Ultimately, moving toward a safer digital society requires a paradigm shift from reactive law enforcement to proactive, community-led techno-legal capacity building. Policymakers, academic institutions, and law enforcement agencies must collaborate to integrate cyber hygiene and legal literacy into mainstream educational curricula, starting from the high school level. By establishing dedicated, tech-enabled support cells at the grassroots and ensuring continuous engagement through periodic workshops, vulnerable demographics can be transformed from passive, fearful targets into confident, resilient digital citizens. Such a holistic, multi-stakeholder approach will not only bridge the existing gender digital divide but also ensure that the constitutional promise of equality and privacy remains fully realized in an increasingly borderless digital world.

Acknowledgment

The researcher gratefully acknowledges the financial support provided by Acharya Nagarjuna University, Guntur under Rashtriya Uchchatar Shiksha Abhiyan (RUSA), Grant for facilitating the research project titled 'Protecting women against digital deviance with a techno-legal system in Andhra Pradesh'. I acknowledge the support of Prof. Uma Vennam, Vice Chancellor, Prof. R. Usha, Registrar, Prof. N. Rajani, Former Registrar, Prof. C. Vani, Coordinator for their support in smooth conduct and timely completion.

References

1. Bhattacharya, S., & Basu, A. (2022). "Cyber violence against women in India: A techno-legal perspective." *International Journal of Cyber Criminology*, 16(2), 112-128.
2. Chaudhary, R., & Sharma, P. (2021). "The rural-urban digital divide in India: Impacts on gender empowerment." *Information Technology for Development*, 27(4), 650-671.
3. Halder, D., & Jaishankar, K. (2016). *Cybercrimes against women in India*. SAGE Publications India. *(Used to support the specific inclusion of modules on cyberstalking, deviance, and statutory rights).*
4. Directorate of Women Safety and Cyber Operations, Andhra Pradesh Police. *Annual Cyber Safety and Security Report*. Vijayawada; 2024.
5. Government of India. *The Information Technology Act, 2000* (No. 21 of 2000). Ministry of Law and Justice; 2000.
6. Indian Penal Code, 1860 (Act No. 45 of 1860).
7. Jaiswal, A., & Sharma, R. Bridging the gender digital divide: Impact of digital literacy initiatives in semi-urban India. *Journal of Information, Communication and Ethics in Society*, 19(3), 345-360; 2023.
8. Kumar, V., & Sita, P. Awareness of techno-legal provisions and cyber rights among women in Andhra Pradesh. *Asian Journal of Women's Studies*, 30(2), 112-130; 2025.
9. Ministry of Electronics and Information Technology (MeitY). *Information Security Education and Awareness (ISEA) Project Report*. Government of India; 2024.
10. National Crime Records Bureau (NCRB). *Crime in India 2025: Statistics*. Ministry of Home Affairs, Government of India; 2026.
11. Patel, S., & Reddy, M. Digital deviance and online victimization of women in contemporary digital spaces. *Cyberpsychology, Behavior, and Social Networking*, 28(4), 255-269; 2025.
12. Shanlax Publications. (2024). *Empowering Women in a Digital World: Overcoming Barriers to Digital Literacy in India*.
13. Kouser, R. et al. (2025). Unmasking the silent threat: Understanding cybercrimes targeting female

students of Kashmir university—a mixed-method analysis. *Journal of Cybersecurity*, 11(1).

14. Dr. Sandeep Kumar, Kumari Mamta Thakur, (2024). Cyber violence against women and children in India: Accessing prevalence, impact and policy. *JETIR*, 11(8), 74-82.