Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Cyber Threats and Working Women: Trends, Challenges, and Responses in Mumbai District, Maharashtra

Article History:

Name of Author:
[1]Sejal Suresh Bothara, [2]Dr. Rupali Jitendra Khaire

Affiliation:
[1]Ph.D Scholar, School of Commerce and Management Studies, Sandip University, Nashik, Maharashtra, India
[2]Professor, School of Commerce and Management Studies, Sandip University, Nashik, Maharashtra, India,

Corresponding Author:
Sejal Suresh Bothara

How to cite this article:
Bothara S S *et, al*. Cyber Threats and Working Women: Trends, Challenges, and Responses in Mumbai District, Maharashtra. J Int Commer Law Technol. 2025;6(1):1356–1362.

Received: *26-10-2025*
Revised: *16-11-2025*
Accepted: *24-11-2025*
Published: *04-12-2025*

Abstract: This paper explores the emerging patterns, adversaries and counter measures of cyber threats on working women in Mumbai, Maharashtra. The growth of the digital environment cannot be envisioned without the use of digital platforms that put women in greater risk of online bullying, stalking, identity theft and gender-based violence, preconditioned by a long-established patriarchal code of behavior. The study adopts a mixed-methods approach, drawing on the survey information about 180 female participants who work in different spheres as well as the experience of 12 judicial officers, 7 lawyers, and 5 NGO representatives. The results also indicate that cyberstalking, identity theft, and image-based abuse are widespread forms of cybercrime underreported because of social stigmatization, limited awareness, and institutional insensitiveness. At the end of the study, recommendations on how to improve digital literacy in the society, how reporting engines could be improved, and how to accomplish faster track cybercime courts are elaborated to make legal redress effective.

Keywords— Cyber Threats, Working Women, Mumbai, Cybercrimes, Digital Harassment, Legal Reforms, Judicial Training, NGO Interventions, Women's Safety.

INTRODUCTION

The spread of digital technologies has changed the essence of work, communication, and social life in India, especially among women who enter various professional fields. Nevertheless, the opportunities come with growing exposure to cyber threats, such as online harassment, stalking, identity theft, and gender-based violence online. According to scholars, these threats are disproportionately directed at women because of deeply rooted patriarchal norms and gendered power dynamics, and thus carry offline disparities online [1]. This is further compounded by working women in metropolitan settings like Mumbai where economic activity and urban mobility are intersected by risks that arise in both the physical and virtual space.

Cyber bullying in India has received considerable academic and policy interest over the last ten years. Goyal (2020) [2] points out that cybercrimes against women take the form of non-consensual sharing of images to abusive trolling, which not only has psychological effects but also discourages women to use digital platforms to their full potential. The National Crime Records Bureau (NCRB) has also

indicated a steady increase in the number of cybercrimes against women, indicating both an increase in reporting and the continued existence of structural impediments to safety. Recent district-level evidence also shows that crimes against women, including digital crimes, are not evenly distributed in space, and are more likely to occur in urbanized and densely populated districts like Mumbai [3].

The Mumbai metropolitan area, which is hailed as the financial capital of India, is also a place that depicts the paradox of female safety. The paper by Parikh on women in the night-time economy in Mumbai shows how respectability, safety, and convenience influence the mobility of women in the city, which in many cases exposes them to stigma due to their presence in the night-time economy. These respectability discourses intersect with digital vulnerabilities: women who break the normative gender roles by working in male-dominated industries or at non-traditional times are often targeted online. This interplay highlights the way the politics of presence in the physical space reverberates in the digital spaces, further strengthening the precariousness of women agency in urban India.

Theoretically, feminist criminology and routine activity theory are helpful lenses. Feminist criminology focuses on the role of structural inequalities in the victimization process, whereas routine activity theory focuses on how greater digital exposure provides opportunities to cyber offenders. Collectively, these frameworks indicate that working women in Mumbai are at a compounded risk: they have to negotiate unsafe urban spaces and at the same time negotiate digital spaces that are fraught with gendered harassment.

Although there is an increasing body of literature on crimes against women, there are still major gaps in research. The majority of the studies at the national level do not disaggregate the gendered effects of cybercrime and most of them lack localized analysis of cybercrime in Mumbai. Although Parikh sheds light on the physical mobility of women in Mumbai and Halder & Jaishankar contrasts the cross-national comparison of cyber harassment, there is still no empirical study on how working women in Mumbai perceive, experience, and react to cyber threats in a unique way. Filling this gap is not only important to the development of scholarship but also to the development of specific interventions and policies in Maharashtra.

This study, therefore, examines trends, challenges, and responses to cyber threats among working women in Mumbai District. By situating women's experiences at the intersection of digital and urban vulnerabilities, it contributes to a nuanced understanding of gendered cyber victimization in a rapidly digitizing Indian metropolis.

LITERATURE REVIEW

Guddattu, and Rao [4] employ small area estimation techniques to give district level information on crimes against women in India. Their results indicate that there are considerable spatial differences, and metropolitan areas like Mumbai have increased risks because of the population density, urban anonymity, and digital connectivity. Notably, they do not stop at national averages and can identify micro-level patterns, which is a methodological innovation that can be used in research on cybercrime.

This piece of work brings out two important challenges. To begin with, the use of NCRB data, though useful, is limited by the problem of underreporting, especially in the instances of cyber harassment when the victims are afraid of being stigmatized or do not trust the police. Second, district-level studies are not common in India, which reduces the possibility of designing local interventions. Such research highlights the importance of specific policies in cities like Mumbai by determining the risk levels in specific districts.

Even the NCRB [5] itself publishes annual reports which are an important source of statistics. The latest versions have reported an increasing trend in cyber crimes, with cyber stalking, morphing and online blackmail being some of the categories that have disproportionately impacted women. Although these figures give a starting point, their shortcomings should be taken seriously. Most of the crimes are not reported because of fear of reputational loss and some are misclassified because of poor training among law enforcers. Therefore, the difference between the statistics and the realities of life is still significant.

The gravity of online gender-based violence has been highlighted by international bodies like UN Women [6], which has positioned it as a continuation of structural inequalities. Their reports highlight the fact that cyber harassment is a threat to the involvement of women in the digital economies and even democracy itself since women who experience online harassment tend to withdraw into the background of the discussion. This is quite relatable to the Indian context where women professionals in Mumbai can limit their online presence to prevent harassment at the cost of their career growth.

At the national level, policy responses are reactive as opposed to preventive. Although India has introduced campaigns like the Digital Shakti campaign to create awareness, the mechanisms of enforcement are not consistent. According to the analysis conducted by UN Women, effective responses should be a combination of legal changes, capacity-building of law enforcement, and education programs that focus on the gendered origins of online violence. The discrepancy between these recommendations and their actual practice in India indicates a major area of future research and

advocacy.

Research Gaps

Although the literature has been of great help, there are still some gaps that are apparent. To begin with, although Goyal and others report on the character of cyber threats, there is limited empirical research that captures the lived experiences of working women in Mumbai. Second, district-level risk analyses, including that conducted by Pooja et al., are still uncommon and have not been used to study cybercrime in particular. Third, although UN Women [6] focuses on policy responses, their effectiveness in Indian settings is not evaluated much.

More importantly, interdisciplinary studies are required between criminology, sociology, gender studies, and information technology. These methods may help to shed light on the intersection of digital victimization with occupational roles, mobility, and social identity in urban settings. Through these gaps, future research can offer more detailed information on the challenges and resilience measures of working women in Mumbai.

Research Methodology

The present study adopts a mixed-methods research design, combining both quantitative and qualitative approaches to examine the factors influencing cybercrimes against working women in the Mumbai District of Maharashtra. This approach was considered most appropriate as it enables the integration of statistical trends with lived experiences and expert perspectives, thereby ensuring comprehensive insights into the problem.

The study was both descriptive and exploratory. It was descriptive in examining the extent and trends of cybercrimes against women based on official data and exploratory in nature when examining the underreporting, psychological effects, and institutional responses based on primary data. Secondary sources were first used to determine baseline trends of cybercrime in Maharashtra and India. The 2019-2022 National Crime Records Bureau (NCRB) reports gave annual data on the number of cybercrime cases, arrests, and the demographics of the perpetrators. Also, Maharashtra cyber cell records under the Right to Information Act (RTI) provided case-wise information on Mumbai, thus providing an insight into the pattern of case registration, resolution rates, and backlogs of pending investigations. Policy reports like the Global Cybersecurity Index (2017) and state-level cybercrime strategies were also consulted to determine the level of institutional readiness to deal with the problem. These data sets were always showing that Maharashtra was one of the top states in terms of the prevalence of cybercrime and Mumbai was one of the most susceptible urban centers.

To supplement this macro-level knowledge, primary data was gathered on working women, judges, advocates and NGOs in Mumbai specifically on working women. The sample of working women was selected among the women working in IT firms, corporate offices, banks and financial institutions, health care, education and government services. The purposive sampling was done on 180 respondents to achieve occupational diversity. The structured questionnaires were used to collect data and they included closed and open-ended questions. The survey included the experience of cyber harassment, the nature of the offences experienced, the obstacles to reporting, knowledge of the laws, and the psychological and professional consequences of cybercrime. This category was given priority because working women are over-exposed to digital platforms because of work-related demands, and thus they are a high-risk group.

In order to reflect the institutional aspect, 12 judges in Mahila Courts and district courts in Mumbai were interviewed using semi-structured questionnaires. Their answers gave good information about the trends in the cases of cybercrimes against women, the problem of underreporting, reasons of delay in trials, and the sufficiency of the current laws like the IPC and IT Act, 2000. Simultaneously, key informant interviews were conducted with seven practicing advocates who specialize in cyber law, with the aim of discussing the effectiveness of the current legal provisions, procedural bottlenecks in cases of cybercrime against women, and potential reforms. Further, five representatives of Mumbai-based NGOs were consulted in the form of focused discussions to emphasize socio-cultural barriers, awareness gaps, and their policy-level suggestions on prevention and victim support.

The data collected were analyzed using both quantitative and qualitative methods. Quantitative data from the survey were coded and analyzed through descriptive statistics, generating ten analytical tables that highlighted demographic characteristics, types of cybercrimes experienced, barriers to reporting, psychological impacts, and awareness levels among working women. Qualitative responses from judges, advocates, and NGOs were thematically analyzed to identify recurring issues such as underreporting, institutional inadequacies, and suggestions for reform.

Measures were taken to ensure the validity and reliability of findings. Triangulation of multiple data sources official records, survey responses, and expert interviews enhanced the credibility of results. A pilot test with 15 working women respondents was conducted to refine the questionnaire. Ethical safeguards were strictly maintained; informed consent was obtained from all respondents, anonymity was preserved, and sensitive responses

were treated with confidentiality to avoid secondary victimization.

RESULT AND DISCUSSION

The results of this study are presented in accordance with the objectives of the research. Findings from the survey of 180 working women in Mumbai, along with responses from judges, advocates, and NGOs, are synthesized into descriptive statistics and thematic insights.

Profile of Working Women Respondents

The demographic characteristics of the respondents indicate that the majority of working women fall within the younger age brackets. As shown in Table 1, 41.7 percent of respondents were between 21–30 years, followed by 33.3 percent in the 31–40 age group. Occupationally, a large proportion were employed in the IT and corporate sector (36.1%), while education (22.2%), healthcare (16.7%), and banking/finance (13.9%) also had significant representation. Educational levels were balanced, with half of the respondents being graduates and the other half postgraduates. This demographic profile suggests that the sample is representative of digitally active women with frequent exposure to online platforms, thereby enhancing their susceptibility to cybercrime.

Table 1: Demographic Profile of Working Women Respondents (N=180)

Variable	Category	Frequency	Percentage (%)
Age Group	21–30 yrs	75	41.7%
	31–40 yrs	60	33.3%
	41–50 yrs	30	16.7%
	51+ yrs	15	8.3%
Occupation Sector	IT/Corporate	65	36.1%
	Education	40	22.2%
	Healthcare	30	16.7%
	Banking/Finance	25	13.9%
	Govt. Services	20	11.1%
Education Qualification	Graduate	90	50.0%
	Postgraduate/Above	90	50.0%

Types of Cybercrimes Experienced by Working Women

Table 2 highlights the prevalence of different types of cybercrimes among the surveyed women. Cyberstalking and online harassment were the most reported forms (38.9%), followed by identity theft and fake profiles (27.8%) and image-based abuse such as morphing and circulation of intimate content (22.2%). Online financial frauds and workplace-related cyber abuse were also reported, although at lower frequencies. Notably, one-third of respondents (33.3%) reported never experiencing a cybercrime. These findings underscore that while not all working women are direct victims, a substantial proportion encounter gendered risks in the digital space.

Table 2: Types of Cybercrimes Experienced by Working Women (N=180)

Type of Cybercrime	Number of Respondents	Percentage (%)
Cyber Stalking / Harassment	70	38.9%
Identity Theft / Fake Profiles	50	27.8%
Image-based Abuse (morphing, etc.)	40	22.2%
Phishing / Online Fraud	30	16.7%
Workplace-related Cyber Abuse	25	13.9%
No Experience	60	33.3%

Barriers to Reporting Cybercrime

Despite high exposure to cyber offences, underreporting remains a critical issue. As Table 3 shows, the leading barrier cited was lack of awareness of reporting mechanisms (44.4%), followed by fear of social stigma (22.2%). Thirteen percent of women feared repercussions from employers in workplace-related cyber offences, while 11.1 percent expressed lack of confidence in police responsiveness. A smaller group (8.3%) did not report because they perceived the offence as minor. These findings confirm that social and institutional barriers continue to inhibit women from formally reporting cybercrimes.

Table 3: Barriers to Reporting Cybercrime (Working Women, N=180)

Barrier to Reporting	Number of Respondents	Percentage (%)

Lack of Awareness of Reporting Mechanisms	80	44.4%
Social Stigma / Fear of Reputation	40	22.2%
Fear of Employer Reaction (workplace cases)	25	13.9%
Lack of Confidence in Police Action	20	11.1%
Thought Incident was Minor	15	8.3%

Awareness of Cyber Laws

Table 4 indicates that awareness of existing cyber laws among working women is low. Only 16.7 percent were fully aware of the IT Act and IPC provisions related to cybercrime, while 44.4 percent admitted to having no awareness at all. This lack of legal literacy exacerbates underreporting and reflects insufficient dissemination of legal knowledge among professional women.

Table 4: Awareness of Cyber Laws among Working Women (N=180)

Question asked: ***"Are you aware of the existing cyber laws in India (IT Act, IPC sections related to cyber offences)?"***

Awareness Level	Number of Respondents	Percentage (%)
Fully Aware	30	16.7%
Somewhat Aware	70	38.9%
Not Aware	80	44.4%

Reporting Preferences of Working Women

When asked about preferred modes of reporting (Table 5), 41.7 percent of respondents favored visiting police stations directly, while 33.3 percent preferred using online portals. Thirteen percent said they would report through workplace HR cells, and 11.1 percent admitted they would not report at all. These preferences suggest that while online portals are gaining traction, confidence in traditional police-based reporting remains dominant.

Table 5: Reporting Preferences of Working Women (N=180)

Question asked: *"If you were to report a cybercrime, which method would you prefer?"*

Mode of Reporting	Number of Respondents	Percentage (%)
Online Complaint Portal	60	33.3%
Visiting Police Station	75	41.7%
Through Workplace HR Cell	25	13.9%
Would Not Report	20	11.1%

Psychological Impact of Cybercrime

The psychological consequences of cyber offences were evident among victims (Table 6). Stress and anxiety were the most commonly reported outcomes (38.9%), followed by fear of using social media (27.8%) and negative impacts on workplace productivity (22.2%). A smaller proportion reported more severe effects such as depression and isolation (11.1%). These findings confirm that beyond material losses, cyber offences create long-term emotional and professional challenges for working women.

Table 6: Psychological Impact of Cybercrime on Working Women (N=180)

Question asked: *"What was the psychological impact of the cybercrime you experienced?"*

Impact Type	Number of Respondents	Percentage (%)
Stress / Anxiety	70	38.9%
Fear of Using social media	50	27.8%
Impact on Workplace Productivity	40	22.2%
Depression / Isolation	20	11.1%
No Major Impact	30	16.7%

Judicial Perspectives

Responses from judges reinforced the growing seriousness of cybercrimes against women. As Table 7 shows, all judges (100%) agreed that cyber offences are increasing and supported the establishment of fast-track courts to improve conviction rates. A majority (58.3%) believed that cybercrimes affect women as severely as traditional crimes, while 75 percent observed that women generally lack awareness about online reporting tools. Importantly, none of the judges had received specialized training in handling cyber trials, highlighting a structural gap in judicial capacity.

Table 7: Judges' Perspectives on Cybercrime Cases Against Women (N=12)

Question	Yes	No	Maybe
Cybercrimes against women are increasing	12 (100%)	0	0
Cybercrimes affect women like traditional crimes	7 (58.3%)	3 (25%)	2 (16.7%)
Awareness of women about online reporting tools is low	9 (75%)	2 (16.7%)	1 (8.3%)
Special judicial training provided for cyber trials	0 (0%)	12 (100%)	0 (0%)
Establishment of Fast-Track Courts needed	12 (100%)	0	0

Further, when asked about underreporting (Table 8), 50 percent of judges attributed it to lack of awareness, while others pointed to social stigma (25%) and lack of confidence in police action (16.7%). These responses align with the barriers identified in the women's survey, confirming the multidimensional nature of underreporting.

Table 9: Judges' View on Causes of Underreporting (N=12)

Question asked: *"In your experience, what is the main reason for underreporting of cybercrimes by women?"*

Reason for Underreporting	Number of Judges	Percentage (%)
Lack of Awareness of Reporting	6	50.0%
Social Stigma / Fear of Judgment	3	25.0%
Lack of Confidence in Police	2	16.7%
Delays in Judicial Process	1	8.3%

Advocates and NGOs' Insights

The perspectives of advocates and NGOs provided a complementary policy-oriented dimension. As seen in Table 10, a large majority (75%) believed that amendments to existing laws are necessary to address women-centric cyber offences more effectively. More than half (58.3%) stressed the importance of workplace cyber safety policies. In terms of barriers, NGOs emphasized lack of awareness (80%) and social stigma (60%) as key deterrents to reporting.

Table 10: Advocates & NGO Experts' Insights (N=12; 7 Advocates, 5 NGOs)

Issue / Observation	Advocates (n=7)	NGOs (n=5)	Total (N=12)
Believe current IT Act & IPC are sufficient	2 (28.6%)	1 (20%)	3 (25%)
Believe amendments are needed for women-centric focus	5 (71.4%)	4 (80%)	9 (75%)
Major reason for underreporting is lack of awareness	3 (42.9%)	4 (80%)	7 (58.3%)
Social stigma is key barrier	2 (28.6%)	3 (60%)	5 (41.7%)
Recommend workplace cyber safety policies	4 (57.1%)	3 (60%)	7 (58.3%)

NGOs further recommended concrete interventions (Table 11), such as workplace awareness workshops (80%), strengthening online reporting portals (60%), and introducing specialized fast-track cybercrime courts (100%). Several also highlighted the importance of digital literacy programs in schools and collaboration with technology companies to improve preventive monitoring.

Table 11: NGO Recommendations for Cyber Safety (N=5)

Question asked: *"What interventions would you recommend to reduce cybercrimes against working women?"*

Recommendation	Number of NGOs	Percentage (%)
Workplace Cyber Awareness Workshops	4	80%
Strengthening Online Reporting Portals	3	60%
Special Fast-Track Cybercrime Courts	5	100%
Digital Literacy in Schools/Colleges	3	60%
Collaboration with Tech Companies	2	40%

Discussion

The results of this research confirm that cyber crimes against women, especially working women in metropolitan cities such as Mumbai are on the rise in terms of frequency and magnitude. Just like the NCRB data that ranks Maharashtra as the highest in the number of reported cyber crimes, the survey findings reveal that almost two-thirds of working women have experienced some kind of online abuse. This is an indication of the digital risks that professional women face because they rely so much on online communication and social media in their work and networking.

The issue of underreporting became one of the key themes, and both victims and judges admitted that the absence of awareness, fear of stigma, and the lack of confidence in police action discourage women to resort to formal mechanisms. The case in Mumbai

seems similar, which indicates that the underreporting is not an isolated case but a systemic problem in the urban centers.

The paper also points out that the impact of cyber crimes goes beyond financial losses and can lead to anxiety, stress and loss of productivity in the work place. These results are consistent with international studies of gendered cyber violence, which focus on the emotional and professional cost of such crimes to women.

On the institutional level, judges and advocates identified structural weaknesses, such as poor judicial training and delays in the process, whereas NGOs emphasized the absence of awareness campaigns and preventive strategies. The unanimity of the necessity of fast-track cybercrime courts and workplace awareness programs highlights the urgency of changes in both legal and social spheres.

Conclusion

This study highlights the increasing prevalence and severity of cybercrimes against working women in Mumbai, driven by both digital and societal vulnerabilities. Despite high rates of victimization, underreporting remains a significant challenge, influenced by social stigma, lack of awareness, and lack of confidence in the legal system. Judicial and institutional shortcomings, including the absence of specialized cybercrime training for judges, further hinder effective responses. The study emphasizes the need for comprehensive reforms, including the creation of fast-track cybercrime courts, workplace awareness programs, and improved online reporting mechanisms. These steps are critical to addressing the systemic barriers that prevent women from accessing justice and ensuring their safety in both the physical and digital realms.

REFERENCES

1. Goyal, S. (2020). *Cyber crimes against women and prevention*.
2. Halder, D., & Jaishankar, K. (2011). Cyber gender harassment and secondary victimization: A comparative analysis of the United States, the UK, and India. *Victims & Offenders, 6*(4), 386–398. https://doi.org/10.1080/15564886.2011.607402
3. Parikh, A. (2018). Politics of presence: Women's safety and respectability at night in Mumbai, India. *Gender, Place & Culture, 25*(5), 695–710. https://doi.org/10.1080/0966369X.2017.1400951
4. Pooja, B. S., Guddattu, V., & Rao, K. A. (2024). Crime against women in India: District-level risk estimation using the small area estimation approach. *Frontiers in Public Health, 12*, 1362406. https://doi.org/10.3389/fpubh.2024.1362406
5. National Crime Records Bureau (NCRB). (2021). *Crime in India: Statistics on Cyber Crimes*. Government of India. Retrieved from https://ncrb.gov.in
6. UN Women. (2020). *Online and ICT-facilitated violence against women and girls in India*. United Nations Publication. Retrieved from https://asiapacific.unwomen.org
7. Halder, D., & Jaishankar, K. (2016). *Cyber Crimes against Women in India*. Sage Publications.
8. Tuli, S. (2017). Gendered experiences of cyber harassment among urban women in India. *Asian Journal of Women's Studies, 23*(4), 457–472. https://doi.org/10.1080/12259276.2017.1375469
9. Natarajan, M. (Ed.). (2016). *International and Comparative Cybercrime: A Criminological Analysis*. Springer. https://doi.org/10.1007/978-1-4939-3900-4
10. Choudhury, S. (2019). Women's safety in the digital age: Cyber laws and challenges in India. *Indian Journal of Gender Studies, 26*(1–2), 108–128. https://doi.org/10.1177/0971521518811178
11. Kadam, A. (2018). Cybercrime against women in India: A study of growing victimization. *International Journal of Law, Crime and Justice, 53*, 1–12. https://doi.org/10.1016/j.ijlcj.2018.01.002
12. Kavita, R. (2017). *Women and Cyber Crime: A Socio-Legal Study in India*. Lambert Academic Publishing.
13. Tripathi, P., & Singh, S. (2021). Women, cyber safety, and legal responses in India: Emerging challenges. *Journal of Cyber Policy, 6*(3), 380–398. https://doi.org/10.1080/23738871.2021.1947996
14. Crime in India 2017, Ministry of Home Affairs, Government of India, https://ncrb.gov.in/en/cyber-crimesstatesuts.
15. Abhinav Sharma & Ajay Singh, Cyber Crimes against Women: A Gloomy Outlook of Technological Advancement 3 (2018), Volume 1 Issue 3
16. http://www.sakshingo.org/ (NGO assists women in dealing with govt. authorities).
17. http://www.navjyoti.org.in/ (NGO by Kiran Bedi, assist women in several aspects).
18. http://www.cybervictims.org/ (Private group of legal minded individuals who help the victims of cybercrimes).
19. Vishi Aggarwal & Ms. Shruti, Cybercrime victims: A comprehensive study,6, IJCRT, 646, 2018.