

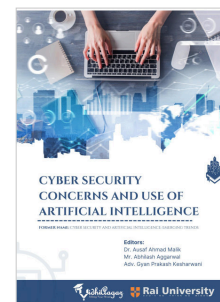
CHAPTER 30

Cybercrime against Women in India: A Comparative Study of Pre and Post-Covid-19 Pandemic Period

Ramesh Chandra Sethi and Arpita Jena

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 250–257

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Ramesh Chandra Sethi & Arpita Jena, *Cybercrime against Women in India: A Comparative Study of Pre and Post-Covid-19 Pandemic Period*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 250 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Ramesh Chandra Sethi and Arpita Jena, 'Cybercrime against Women in India: A Comparative Study of Pre and Post-Covid-19 Pandemic Period' in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 250.

CHICAGO (17TH ED.)

Sethi, Ramesh Chandra, and Arpita Jena. "Cybercrime against Women in India: A Comparative Study of Pre and Post-Covid-19 Pandemic Period." In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 250–257. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-30/>.

APA (7TH ED.)

Sethi, R. C., & Jena, A. (2024). Cybercrime against women in India: A comparative study of pre and post-covid-19 pandemic period. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 250–257). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-30/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-30/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CYBERCRIME AGAINST WOMEN IN INDIA: A COMPARATIVE STUDY OF PRE- AND POST-COVID-19 PANDEMIC PERIOD

Dr. Ramesh Chandra Sethi⁴³ and Arpita Jena⁴⁴

ABSTRACT

Background: The COVID-19 pandemic has created havoc in all Nation-States worldwide. The transmission of the virus led to an increase in cases that led to the global imposition of lockdown. This situation forced a large number of people confined within four walls, including women, to be engaged in surfing the internet (i.e., the use of the internet and various social media platforms) during the pandemic. As stated by the National Crime Records Bureau (NCRB), the Government of India, there is an increasing number of cybercrime cases against women from 8,415 (2019) to 10,405 (2020), and it further jumped to 10,730 cases in 2021 during COVID-19. It indicates that heavy browsing of the internet led to a significant increase in Cybercrimes Against Women (CAW) during the pandemic.

Objectives: (i). To critically analyze the root causes of cybercrimes against women in India; (ii) To scrutinize various judicial pronouncements related to CAW. (ii). To critically investigate and examine the data published by the National Commission for Women (NCW) and to find out the trends of CAW in India before and after the pandemic.

Methodology: This study is based on doctrinal research of secondary data sources followed by qualitative and quantitative research methods.

Findings: The findings suggest that the imposition of lockdown has increased CAW due to their active engagement in the digital world. The study also reveals that educated, tech-savvy women living in cities are more prone to victims of cybercrimes.

Conclusion: India has adopted various stringent laws to prevent cybercrimes. However, due to a lack of awareness, effective and efficient rule implementation, and robust monitoring mechanisms, the government has failed to ensure a crime-free society for women even after 78 years of independence.

Keywords: COVID-19 pandemic, women, cybercrime, technology and legislation.

INTRODUCTION

The 'COVID-19' had a profound effect on all facets of life. To tackle its spread, the government of India had enforced a complete lockdown measure across the country. As a result, people are confined within four walls without any work. The isolated life with no work and other engagement has forced people, specifically young women, to surf the internet (i.e., the use of the internet for different purposes, including online shopping and use of various social media platforms) during the pandemic. The large volume of internet users ultimately falls into the trap of 'cybercrime' (Mondal and Paul, 2022). The victims of this crime are mainly women because there is a growing number of women who depend on online sources for a variety of purposes, which include employment, education, purchasing goods and availing services, personal and social contacts, entertainment, and related operations etc. The more time they spend on the internet, the probability of more cyber fraud they face, and the offenders get more

⁴³ Assistant Professor at School of Law, Kalinga Institute of Industrial Technology (KIIT), India.

⁴⁴ Student at School of Law, Kalinga Institute of Industrial Technology (KIIT), India.

opportunities for committing cybercrime. According to UN Women's research, the global surge in internet use throughout the 2020 pandemic has led to a spike in reports of virtual abuse against women. It was mentioned that as women spend most of their time virtually so, there is a higher chance of experiencing virtual harm, such as threatening and defamatory content, as well as sexual abuse messages and sexual violence, which ultimately leads to an increase in cybercrime. Therefore, the UN has termed the 2020 pandemic a 'Shadow Pandemic'.

Furthermore, 'Online Gender-based violence against women (Online GBVAW) is defined as any act of GBVAW that is committed, assisted or aggravated in part or fully by the use of information and communication technologies (ICTs) such as smartphones, internet, social media platforms or email, against a woman which led to the growth of crime against them disproportionately.' When it comes to a spectrum of various, recurrent, and connected types of violence based on gender, it was found that women experience more virtual abuse than men while accessing the internet. Social networking sites should not be a place of safety and security for women, though they have become essential to their lives in this digital age. Women often self-censor in response to online harassment they face, either by stopping the use of social media altogether or drastically cutting back without going and reporting the incident to an appropriate authority. This simply highlights the fact that women cannot exercise their Constitutional rights to 'freedom of expression and a dignified life,' as stated in 'Articles 19 and Article 21' of the Indian Constitution. It was further observed that the psychological effects of online harassment are severe, and women feel insecure utilizing cyberspace. They also hesitate to get legal support because of insecurity and societal stigma. As per the data of the UN, it was observed only 10% of the women who were victims registered their complaints at the police station. In contrast, 90% of women still hesitate to take legal protection due to societal stigma and personal dignity.

Further, as per the National Crime Bureau Report (NCBR, 2020), it was held that there is a 24% decrease in all crimes related to women, but simultaneously, there is a 54% increase in cybercrime among women. These data showed that the rise in dependency on the internet led to a severe increase in cybercrime against women. Though the Parliament of India has made thousands of laws for protecting women, their negligence of not disclosing the cases/crimes has led them to be more prone to cybercrime. To reduce cybercrime, there is a need for adequate awareness and combining efforts along with stringent laws to fight against cybercrime, making India a better place for the safety and security of women.

METHODOLOGY

This study is qualitative doctrinal research. The data are collected from various secondary sources, and other relevant information is available in multiple publications, documents, and reports of the Government of India and national and international institutions/ organizations. Furthermore, the study analyzes the trends of increasing cybercrime, as per the data given by NCBR and the analysis of data provided by each State regarding various cybercrimes against women.

CAUSES FOR CYBERCRIMES

(i) Judicial reasons

The preamble of the IT Act of 2000 shows its primary goal is to enhance e-commerce. Enhancing e-commerce encompasses business and economic offenses such as fraudulent activity, violation of confidentiality, and malware that steals confidential information. The S.66,67,72 of the IT ACT, 2000 deal with these things. These three sections deal with everything except e-commerce offenses. Whereas there is an increase in the number of crimes related to women, like cyberbullying, cybersex, etc., that are not dealt with specifically under the IT Act, the IPC and the Indian Constitution give protection against crimes such as rape. Outraging the modesty of women, they also fail explicitly to provide security to women related to cybercrime. Following the '2012 Delhi gang rape case (Nirbhaya Case)', there has been a significant public uproar calling for new laws and regulations to be implemented to safeguard women from criminals. 'Sections 354, 354 A, 354 B, 354 C, and 354 D' are among the changes to the IPC made possible by the 2013 Criminal Law Amendment Ordinance.

(ii) Societal reasons

The majority of cybercrime increases because the victim hesitates to disclose the crime as she fears her family's reputation will be damaged. She firmly believes that she will be blamed and her dignity will be destroyed in society. As a result, she does not disclose the crimes committed to her. Women are more susceptible to cybercrime because the criminal's identity is unknown, and he may use fake identities and persistent threats to harass the victim. Women are worried that coming forward with the crime and complaining in an appropriate forum might make lives more difficult. They are also in a dilemma, whether their friends and relatives will stand by and support them or not. They are also worried about the effect the after-event will have on society. Owing to these anxieties, women frequently neglect to report crimes, which raises the morale of those who commit them and increases cybercrime significantly in India.

(iii) Easy accessibility by the perpetrator

When we discuss crimes, we typically consider aggressive offenses involving bodily harm/injury. To commit such crimes, we often need to perform some physical labor and create a plan to carry out such action with a weapon. However, that is the opposite when it comes to cybercrime. In this case, a person can be a perpetrator by simple devices in the modern world. Cybercrime can occur anywhere without a territorial nexus, making it much easier to commit than other physical crimes.

(iv) Increase of male users in social media as compared to females

Research states that most internet users are male on any social networking platform. As per the data of the IT Department, it was found that around 73% of users are male compared to females. This can be another reason why women are the target when a large number of male members are on these platforms, as they strictly go by the patriarchal mindset. Even today, many male members think women should not be using social media sites. Hence, this notion of patriarchy may lead to several agonies, which ultimately results in cybercrime.

JUDICIAL PRONOUNCEMENT

(i) **“Manish Kathria v. Ritu Kohli”** - is the first related cyberstalking case. In this instance, Mrs. Ritu Kohli reported to the police that someone had been employing her personal information to speak online at ‘<http://www.micro.com/>,’ primarily in Delhi. The police looked into the case in detail and apprehended the perpetrator. Further, the individual used her identity, provided her address, and engaged in vulgar behavior when communicating online. Additionally, the same individual purposefully provided other participants with her phone number, urging them to give her a call at additional hours. As a result, she received nearly 40 calls in three days during the additional hours. These calls created an agony in her private life. Furthermore, the IP access of the culprit was found by the police, and then the culprit was arrested. Subsequently, the case was registered, but unfortunately, the culprit was bailed and released. The cyber laws in India do not address cyberstalking. The only area where an individual can be charged remotely for violating privacy and secrecy under Section 72 of the IT Act. The culprit could be additionally charged under Section 441 of the IPC and Section 509 of the IPC.

(ii) **“State of Tamil Nadu v. Suhas Katti”**: In this case, the accused person created a fictitious e-mail ID of the victim’s identity and forwarded communications to the divorced woman to obtain details. The victim experienced psychological assault as a result of the publication of comments as she continues to receive bothersome phone calls. As a result, in February 2004, she complained to the Egmore Court and the Cyber Unit of the Tamil Nadu Government. The Cyber Unit took the accused person into custody. He was charged under Sections 67 of the IT Act of 2000 and 469/509 IPC after proving that he had committed an offense.

(iii) **“Avnish Bajaj v State of (N.C.T) of Delhi”**: A customer-to-customer company called Baze.com was discovered to be selling MMS recordings under the guise of “DPS girls having fun.” The chief executive officer of the sales company, Avnish Bajaj, was detained, and his request for release was denied. The IT Act of 2000's section 67 led to his detention. The defendants in the present instance argued that section 67 of the Act deals with the printing and distribution of pornographic material rather than its delivery. The court ruled that the real pornographic video or clip could not be viewed on the Baazee.com platform. The court granted the offender bail alongside a one lakh surety.

COMPARATIVE SCENARIO OF CAW IN PRE- AND POST-COVID PANDEMIC PERIOD

Table-1 and Figure-1 (given below) show the crime against women before, during, and after COVID-19 from 2018-2023. It was observed that 49953 CAW were committed in the last five years (2018-2023), out of which 6030 crimes were registered in 2018-2019, followed by 8379 cases in 2019-2020, and in 2020-2021, there was a sudden 20% (10405 cases) increase in CAW due to the complete lockdown and all including women were confined within four walls and ordered all essential commodities from the online sources for their day-to-day activities. Therefore, women are more vulnerable to cybercrime. Furthermore, the lockdown boosted the number of individuals meeting online, which has raised the prevalence of online pornography to 1655 in 2020-2021 from 1174 in 2019-2020, and digital stalking increased to 887 in 2020-2021 from 785 in 2019-2020. Similarly, other types of cybercrimes, namely morphing (251 cases), cloned profile (354 cases), and other crimes (7184 cases

in 2020-2021 from 5995 in 2019-2020) against women also increased significantly (see Table-1) during 2020-2021 post COVID-19 pandemic period. This happened because of the absence of knowledge of legal procedures, lack of consciousness, and inadequate cybersecurity protections, which led to women being targeted by hackers. The majority of perpetrators of cybercrime are women, which has been sharply increasing day by day. The COVID-19 shutdown has contributed to a boost in cybercrime incidences nationwide. About 10,405 CAW cases were formally recorded in 2020-2021, per the (NCBR). Table-2 shows that around 49953 cybercrimes were committed against women between last five years from 2018 to 2023. In 2022-2023, around 27.09% of cybercrimes against women were committed in Karnataka, compared to 22.07% in 2018-2019. This trend shows a 3% increase in cybercrime, making Karnataka a more prone State to CAW. So, the State of Karnataka recorded the highest number (13078 cases in Karnataka alone) of CAW followed by Maharashtra (8624 cases), Assam (3910 cases), Uttar Pradesh (3666 cases), Telangana (3418 cases) and Odisha (2373 cases) in the country. Besides analyzing data, CAW in India continues to be overlooked as a serious issue. Typical internet extortion techniques being used against women include objectification, defamation, picture morphing, harassment, and demanding cash as compensation for sating sexual desires. Women's confidence in utilizing networking sites and the World Wide Web has also been damaged, and there is now a real risk to their safety and anonymity. Hence, it can be concluded that women are more prone to cybercrime. While it is evident that ever since the pandemic in India, cybercrime has caused considerable harm, various reasons have exacerbated the problem and increased cybercrime cases. Undoubtedly, the internet has benefited human civilization in many ways, but simultaneously, it also causes harm to society at large.

Table-1: Types of Cybercrime Against Women

Types of cybercrime	2018-2019	2019-2020	2020-2021	2021-2022	2022-2023	Total
Threatening	113	132	74	200	125	644
Pornography	862	1174	1655	1896	2251	7836
Stalking	738	785	887	1172	1457	5039
Morphing	62	65	251	276	385	1039
Cloned profile	207	288	354	225	179	1253
Other crimes	4048	5995	7184	6961	9870	34058
Total cybercrime against women	6030	8379	10405	10730	14409	49953

Source: Crime Report 2018 to 2023, NCBR, New Delhi

Figure-1: Types of Cybercrime Against Women

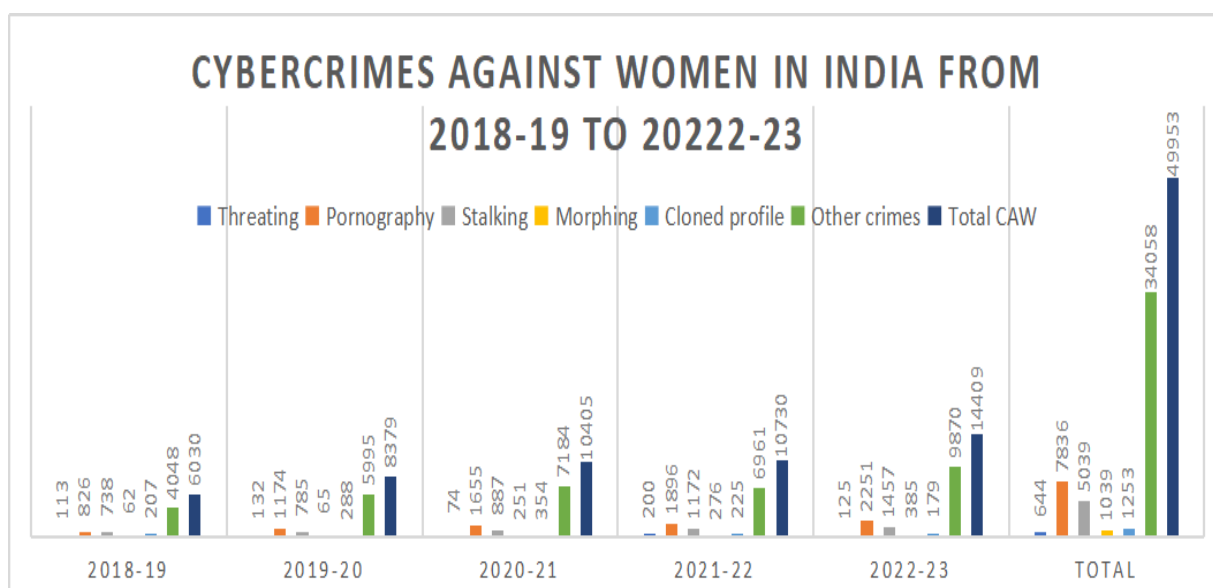


Figure-2: State-wise Cases of Cybercrime Against Women in India

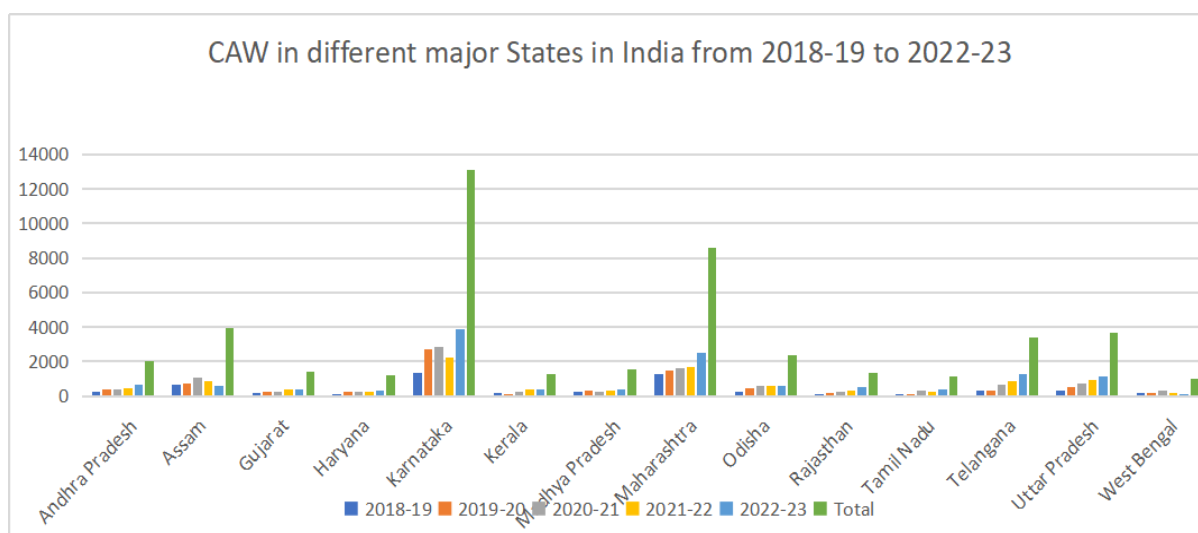


Table-2: State-wise Cases of Cybercrime Against Women in India

State/ UT	2018-19	2019-2020	2020-2021	2021-2022	2022-23	Total
Andhra Pradesh	217	356	375	471	637	2056
Arunachal Pradesh	1	5	1	16	5	28
Assam	670	703	1071	856	610	3910
Bihar	14	60	47	56	84	261
Chhattisgarh	64	85	117	194	279	739
Goa	21	5	19	15	32	92
Gujarat	184	226	277	349	352	1388

Haryana	112	251	222	266	327	1178
Himachal Pradesh	52	47	52	39	46	236
Jharkhand	13	43	20	70	106	252
Karnataka	1374	2698	2859	2243	3904	13078
Kerala	160	139	246	353	381	1279
Madhya Pradesh	276	301	274	298	390	1539
Maharashtra	1262	1503	1632	1697	2530	8624
Manipur	9	2	26	39	13	89
Meghalaya	32	21	39	21	27	140
Mizoram	4	2	1	13	0	20
Nagaland	2	1	2	1	1	7
Odisha	228	437	560	574	574	2373
Punjab	97	87	110	179	194	667
Rajasthan	116	188	238	297	498	1337
Sikkim	1	1	0	0	11	13
Tamil Nadu	77	124	306	248	401	1156
Telangana	336	288	649	883	1262	3418
Tripura	5	3	3	1	4	16
Uttar Pradesh	340	518	749	958	1101	3666
Uttarakhand	78	28	72	183	161	522
West Bengal	170	170	344	201	142	1027
A&N Islands	5	2	3	3	12	25
Chandigarh	5	13	10	12	16	56
D & N Haveli	0	2	3	2	2	9
Daman & Diu	1	0	2	2	3	8
Delhi	79	56	51	151	250	587
Jammu & Kashmir	23	14	25	39	39	140
Lakshadweep	3	0	2	0	0	2
Puducherry	0	0	0	0	15	15
Total	6030	8379	10405	10730	14409	49953

Source: Crime Report 2018 to 2023, NCB, New Delhi

CONCLUSION

In India, women's safety and security has been neglected due to the patriarchal nature of the society. At the same time, there is lack awareness for legal entitlements and women empowerment. All forms of crimes against women are on the rise, but becoming a target of cybercrime is perhaps the most painful experience for a woman. It is not only highly prevalent in India but also around the world. During the outbreak of 2020 COVID-19 pandemic, more women are forced to use the services of the internet and it resulted in the effects on their emotional, interpersonal, and physical wellness as well as a higher likelihood of digital bullying and intimidation of the victims. The pandemic was a period when women were more vulnerable to cyberbullying due to their growing reliance on electronics gadgets. It also highlighted the need to foster an atmosphere of distrust to avoid the abuse of information and data privacy. Although, India has implemented IT Act, 2000 to combat cybercrime but this IT Act has not successfully addressed the critical issues pertaining to the privacy and protection of women. The majority of instances of cybercrime remains unreported because Indian women are either ignorant of it or afraid of it. This kind of ignorant and soft attitude provide opportunities to the criminals to go away after committing the cybercrime. Many private and public websites and other online platforms offer security advice for women's online safety. Hence, proper awareness along with combining effort and strict implementation of laws specifically dealing CAW can help in combating CAW and to make India a better place for women's safety, security and provide a sustainable world for the women.

REFERENCES

- Rathor and Das, "Cyber Crime: The Emerging trends and challenges", CyberSpace and Law : Issues and Challenges, NALSAR University, Hyderabad, 2004 p. 102.
- Snook A., "Stalking in the workplace the complete guide to prevention and investigation", available at: <https://www.i-sight.com/resources/stalking-in-the-workplace-the-complete-guide-to-prevention-and-investigation>
- Dr. Mrs. K. Sita Manikyam, Cyber Crime – Law and Policy perspectives, 40 (Hind Law House, Pune, 2009).
- Cyber Crimes and the law, Legal India, legalnews and law resource portal (Mar 30,2024,03:21 PM), available at <http://www.legalidia.com/cyber-crimes-and-the-law/>.
