INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN(O): 2455-0620 [Impact Factor: 7.581]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 9, Issue - 7, July - 2023 Publication Date: 31/07/2023

DOIs:10.2015/IJIRMF/202307043 --:-- Research Paper / Article / Review

Analysing the Impact of the Pareto Principle on Cyber Crimes against Women during the COVID-19 Pandemic in Maharashtra: Challenges and Remediation Strategies

[1]Ms. Trushna G. Bansod, [2]Dr. Varsha N. Deshmukh
[1]Research Scholar, Dr. Panjabrao Deshmukh College of Law, Amravati, India
[2]Principal, Dr. Panjabrao Deshmukh College of Law, Amravati, India
Email - [1]trushnabansod@gmail.com

Abstract: *The COVID-19 pandemic brought unprecedented challenges to society, with people increasingly relying on digital platforms for communication, work, and leisure. Unfortunately, this shift also led to a surge in cybercrimes, affecting vulnerable groups such as women. This research article examines the application of the Pareto principle (80/20 rule) to identify the most common types of cybercrimes faced by women in Maharashtra during the pandemic. This research examines the prevalence and consequences of cybercrimes faced by girls and women, with a focus on incidents involving WhatsApp on Android phones. Among college girls, 56.5% experienced cybercrimes, with 78.6% of cases involving known perpetrators, often from their workplaces. After incidents, 35.7% blocked and reported the accused, while 7.1% took no action. Surprisingly, 11.1% lacked belief in the cybercrime department's effectiveness. Emotional stress and mental agony affected 36.4% of victims, and 7.1% attempted suicide due to cybercrimes. Though 72.7% reported no routine disruptions, 18.2% had to halt education. Perpetrators were mainly young males, with rural areas being prevalent, yet no convictions were observed, and victims lacked government compensation.*

Key Words: *Cyber Crime, Women, COVID-19 Pandemic, Maharashtra.*

1. INTRODUCTION:

The COVID-19 outbreak accelerated the shift to a digital lifestyle, leading to a surge in cybercrimes, especially affecting women (Lassies) with increased online harassment, identity theft, and cyberstalking.[1-2] Cybercrime continues to grow despite reduced mobility during the pandemic, highlighting the need for intervention strategies.[3] The rapid growth of social media platforms has contributed to an increase in cybercrimes, as cybercriminals exploit these platforms for phishing, identity theft, and cyberbullying. During the COVID-19 pandemic, the use of electronic devices surged as people relied on technology for remote work, online education, and virtual social interactions.[4] Electronic devices played a crucial role in facilitating communication, entertainment, and access to essential services during lockdowns and social distancing measures (Fig. 1).

Figure 1: Electronics devices.

Cybercrime encompasses a wide range of illegal activities conducted through computer networks or digital devices. One category of cybercrime involves crimes that violate personal or corporate privacy, such as invading digital repositories and using illegally obtained information to intimidate individuals or businesses. Personal information theft is also on the rise and poses a significant concern for individuals and organizations alike. As computers and the Internet continue to play a central role in various aspects of society, cybercrime, particularly over the Internet, has become increasingly prevalent, leading to sporadic growth in global cyber threats.[5] The anonymity and wide reach of social media provide fertile ground for spreading malware and misinformation, making users vulnerable to various cyber threats (Fig. 2).

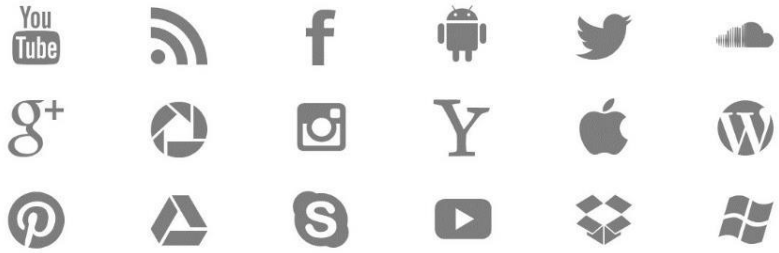


Figure 2: Social medias.

Cybercrime can be classified into several categories based on the nature of the crime and the target of the attack. The three main categories are individual, property, and government crimes, with the latter often referred to as cyber terrorism. Individual crimes involve various acts like ATM fraud, credit card fraud, and telecommunications fraud. Property crimes often involve the use of computers to aid in criminal activities, such as drug offenders using technology for money laundering and trafficking.[6] The fourth category encompasses newly emerging crimes related to the proliferation of computers, such as software piracy, alcohol smuggling, and theft of computer equipment. Fraud and financial crime are specific forms of theft where deception, manipulation, or abuse of trust is employed to gain monetary or property benefits illegally. These crimes can take various forms in today's complex economy, including counterfeiting, credit card fraud, embezzlement, and money laundering.[7]

Victims of financial crimes need to be vigilant and report such incidents to appropriate authorities as soon as possible to mitigate further damages. One prominent form of cybercrime is computer fraud, which involves dishonest misrepresentations of fact intended to deceive others and result in personal gain. Reporting such fraudulent activities to law enforcement agencies is crucial to preventing further harm. The victims of cyber fraud should also dispute any fraudulent charges and gather relevant documents, such as bank statements and tax returns, throughout the reporting process to support their case effectively.[8] Specific types of cybercrime include identity theft, where personal financial information is stolen and used for fraudulent withdrawals or opening fake accounts; investment fraud, where false information is used to sell deceptive investments or securities; mortgage and lending fraud, involving fraudulent mortgages or loans using victim's information; mass marketing fraud, conducted through spam emails or phone calls to steal personal financial information or solicit contributions for fake organizations; and telecom fraud, where criminals use deception over the phone to trick victims into parting with money.[9]

Maharashtra is a state located in western India, known for its rich cultural heritage and economic significance. With a population of over 120 million people, Maharashtra is the second-most populous state in India, contributing significantly to the country's diverse demographics. The state of Maharashtra is divided into 36 districts and is geographically divided into six regions, namely Western Maharashtra, Konkan, Vidarbha, Marathwada, Khandesh, and Northern Maharashtra (Fig. 3).[10] The Pareto principle was applied to identify prevalent cybercrimes in Maharashtra. Technology's benefits bring security and privacy challenges, while youth face online risks like cyberbullying and addiction.

2. LITERATURE REVIEW:

The literature survey on cyber crimes during the COVID-19 pandemic reveals a surge in online fraudulent activities, such as phishing and scams, targeting vulnerable individuals adapting to remote work and increased internet

usage.[11] Therefore, an attempts were made to study the condition of cyber crimes against Women during the COVID-19 Pandemic in Maharashtra and further to study the challenges and remediation strategies.

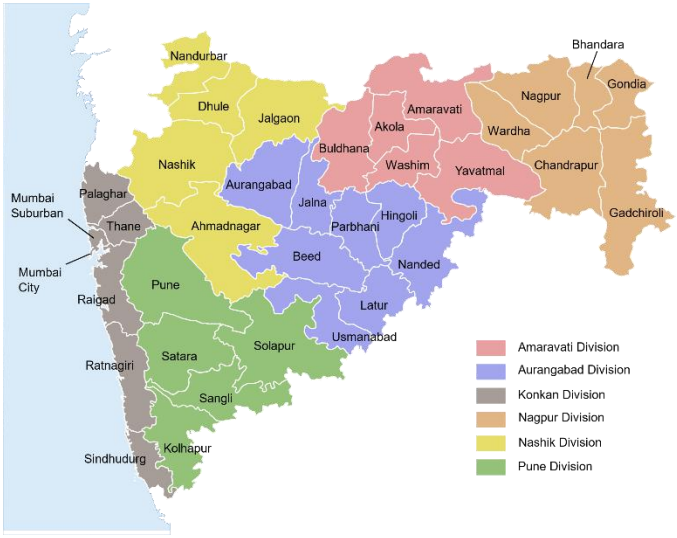


Figure 3: List of districts and division of Maharashtra.

3. METHOD:

A study was conducted for the period of January 2021 to January 2022 to explore girls' views on cyber crimes and ways of enhancing awareness about cyber crimes. The study was composed of two parts: (i) an online survey collected data anonymously from girls belonging to Amravati district, and (ii) information about cyber crimes was obtained from the Crime Investigation Cell of Amravati Police. The main objective of the study was (1) To collect data from girls and women anonymously, ensuring the confidentiality of the survey questionnaires and keeping the questions distinct from each other. Data was gathered without asking for names, addresses, or mobile numbers and (2) To collect data about the number of cases registered so far, types of cyber crime, age group of youngsters who committed crimes, and age of victims from the Cyber Crime Investigation Cell of Districts.

Thoroughly researched and interpreted data revealed the main reasons behind young people's involvement in cybercriminal activity. The collected data, using various methods, can be used to develop an efficient framework and timely preventive measures for societal safety. Statistical tools like Pareto analysis and cluster analysis were applied to enhance the efficacy of the work. Demographic characteristics of the samples were analyzed, and the data was statistically weighted to represent the correct population proportions. Data was collected from 2,300 girls/women (aged 15-35) through an online survey consisting of 31 questions. Additionally, information was obtained from 36 Cyber Cell Officers through telephone interviews, covering 5 questions.

On-line Questionnaires (Multiple choice based) –

Q1. What is your age?
(A)Between 15-20
(B) Between 21-25
(C) Between 26-30
(D) Between 31-35
Q2. Which place do you belong?
(A) Rural
(B) Urban
Q 3. What Is Your Marital Status?
(A) Single
(B) Married
(C) Divorced
(D) Widow
Q4. What do you do?
(A) Take education
(B) Have own business/Work in a Private or government firm

(C) Have left/completed the education and do house hold work
(D) Married and is a home maker

Q5. Which electronic device you have?
(A) Non android Mobile
(B) Android Mobile
(C) Laptop
(D) Both android mobile and laptop

Q6. Which digital social media is used mostly by you-
(A) WhatsApp
(B) Facebook
(C) Instagram
(D) Email
(E) Other

Q7. Have any one created your fake account on social media and tried to defame you?
(A) Yes
(B) No/Never

Q8. Did anyone used your pictures from social media account and misused it by morphing (morphing-paste your picture at some other face, place etc) or posted your humiliating pictures, and threatened or blackmailed?
(A) Yes
(B) No

Q9. Did anyone stalked to you by using digital media (Repeated, unwanted phone calls, texts, messages, etc.)?
(A) Yes
(B) No

Q10. Have you faced Social Media Bullying or Cyber bullying and lost some money?
(A) yes
(B) No

Q11. Have anyone hacked your Social Media account?
(A) Yes
(B) No

Q12. Did someone tracked you by using this social media platform?
(A) Yes
(B) No

Q13. Have any one sexually harassed you by sexting you or intimidated you on any of the digital platform?
(A) Yes
(B) No

Q14. Did anyone bullied you in marriage proposal on matrimony app by using the social media account?
(A) Yes
(B) No

Q15. Did anybody send harassing messages (via text or Internet) or posted disparaging comments on a social networking site in order to harm your reputation?
(A) Yes
(B) No

Q16. Which social media account was commonly used by the person to harass you?
(A) WhatsApp
(B) Facebook
(C) Emails
(D) Instagram
(E) Other

Q17. Any of the above mention act was done by the person who was-
(A) known
(B) Unknown

Q18. The above mentioned acts or another act related to cyber crime by done by a known person who___
(A) Belongs to work place
(B) Belongs to Family
(C) Belongs to friend circle

(D) Belongs to area where you live

Q19. If the person belongs to work place or business, he was your-

(A) Boss
(B) Colleague
(C) Was a worker/labour/peon, etc
(D) any other related to work place

Q20. If the person belongs to Family or close to you, he was your-

(A) Husband
(B) Relative (Brother, uncle etc)
(C) Boyfriend
(D) other

Q21. What did you do after being victim of any such act on social media?

(A) Blocked the account of person
(B) Blocked the account of that person and Informed your parents
(C) Blocked the person and Launched a complaint in cybercrime department
(D) Deleted own account or stopped using that social media account
(E) Took no action

Q22. No action was taken against the person who harassed you on the social media because-

(A) your family didn't allow you to launch a complaint or You were afraid of notoriety in the society (Badnami)
(B) you were not prepared mentally to launch a complaint so you just neglected the act
(C) You were afraid that the person harassing you will torture you more if you complain
(D) The person harassing belonged very close to you and you wished to neglect or cover up his act.
(E) You didn't believe in the cybercrime department

Q23. What was the consequence of such crime on your mental health?

(A) Felt emotional trauma like anger, fear, sadness, nightmares etc
(B) Felt emotional stress like shock, helplessness, trauma etc
(C) Felt as if trapped in web of social media
(D) Felt insecure and always in stress of someone following you
(E) Didn't felt anything

Q24. What was the consequence of such cyber crime on your family?

(A) Family suffered financial loss
(B) Family members also suffered mental agony
(C) Family suffered defamation in society
(D) No effect on family

Q25. What was the consequence of such crime on your social status?

(A) Caused Loss of reputation in society
(B) Felt insecure socially
(C) Felt to get isolated socially
(D) No effect on social image

Q26. What was the consequence of social media crime in your life?

(A) Have to stop the education or change the institute
(B) Have to change or quite the job
(C) Have to leave the place where you live
(D) Suffered a relationship loss
(E) No effect in life

Q27. What you did after being victim of social media media crime?

(A) Stopped using social media
(B) Continued using social media
(C) Use social media but could not trust anyone on digital platform
(D) None of the above

Q28. Did you take any step like trying to commit suicide or harming yourself from mental agony faced due to harassment on social media?

(A) Yes
(B) No

Q29. What you think now after being victim of social media?
(A) Loss of trust on social media
(B) Social media makes one vulnerable for cyber crime
(C) Social media is not trust worthy and keep your information unsafe
(D) Social media is trust worthy and keep your information safe
(E) None of these
Q30. How did you recovered from the mental agony caused to you?
(A) Took medical help
(B) Took spiritual help
(C) Took help of councillor
(D) Took self-efforts to forget the crime caused
(E) Didn't do anything
Q31. Do you feel safe while using social media?
(A) Yes
(B) No

Questionaries for Cyber Crime Investigation cells
Q1. How many cyber crime cases were reported from January 2021 to December 2021?
Q2. How many criminals were in the age group of 15-35?
Q3. What is percentage of cases in which the age of girls and women is 15-35?
Q4. How many accused were convicted in this year?
Q5. Did the victim get any compensation?

4. DATA ANALYSIS:

The collected data was categorized according to different cybercrime types, and the Pareto principle was applied to identify the major categories that contribute to 80% of the total reported incidents.[12]

5. RESULTS AND DISCUSSION:

The survey included 2300 female participants, predominantly young individuals. The data from the cybercrime survey highlights the following key points-

5.1. Cybercrime Survey and Case Data

(1) Age Ratio: The data reveals that the majority of female participants (65.2%) affected by cybercrimes belong to the age group of 21 to 25 years, indicating that youngsters are more vulnerable to such crimes. This could be attributed to their higher usage of digital devices and engagement on various online platforms.

(2) Place Ratio: Cybercrimes are more prevalent in urban areas (60.9%) compared to rural areas (39.1%). The higher incidence in urban areas can be attributed to increased technology usage, better internet connectivity, and higher digital exposure in urban settings.

(3) Marital Status Ratio: Unmarried females (87.9%) are more susceptible to cybercrimes, suggesting that single individuals may be more active on social media and digital platforms, making them potential targets for cybercriminals.

(4) Educational Status Ratio: The data shows that 56.5% of the victims are students, indicating that youngsters who are primarily engaged in educational activities and exploring technology are more likely to be victims of cybercrimes.

(5) Electronics Device Ratio: The data indicates that 52.2% of victims use Android mobile devices, and 47.8% use both Android mobile and laptops. This highlights the prevalence of cybercrimes on mobile platforms, as they are easily accessible and widely used by youngsters.

(6) Digital Social Media Ratio: WhatsApp is the most commonly used social media platform among victims (78.3%). This aligns with the current trend of WhatsApp being widely popular among youngsters, making it a common platform for cybercrimes.

(7) Response on Fake Accounts: 9.1% of participants faced defamation due to fake social media accounts created on digital platforms. This indicates the potential harm caused by cybercriminals using fake accounts to defame and tarnish the reputation of individuals.

(8) Response on Morphing and Blackmailing: 4.3% of participants were victims of threatening or blackmailing through morphing or posting humiliating pictures on social media accounts. This highlights the severe emotional distress and humiliation caused by such cybercrimes.

(9) Response on Stalking: 21.6% of participants were victims of stalking through digital media. Cyberstalking can cause significant mental torture and harassment to the victims, affecting their overall well-being.

(10) Response on Social Media Bullying and Loss of Money: 4.3% of participants experienced social media bullying or cyberbullying, resulting in financial losses. This shows that cyberbullying not only impacts victims emotionally but can also lead to financial consequences.

(11) Response on Hacking of Social Media Account: 13% of female participants reported being victims of social media account hacking. This form of cybercrime can lead to severe consequences, as the hacked accounts can be used to defame and spread false information about the victims, tarnishing their reputation in society.

(12) Response on Tracking of Social Media Account: 8.7% of participants experienced tracking of their social media accounts by the accused. This intrusive form of cybercrime invades the victim's privacy and can lead to feelings of vulnerability and distress.

(13) Response on Sexting-related Sexual Harassment: 8.7% of female participants reported experiencing sexual harassment through sexting on social media. This type of cybercrime not only violates the victim's privacy but also causes humiliation and distress.

(14) Response on Bullying in Marriage Proposals on Matrimony App: 13% of female participants were victims of bullying on matrimony apps, where the accused used social media accounts for harassment. This indicates that even matrimonial platforms are not immune to cyberbullying, leading to emotional distress and negative consequences for victims.

(15) Response on Harassing Messages and Disparaging Comments: 9.1% of participants faced cybercrimes such as receiving harassing messages or disparaging comments on social networking sites. These acts can harm the victim's reputation and cause emotional trauma.

(16) Response on Commonly Used Social Media Accounts by Perpetrators: According to responses, 57.1% of the accused used WhatsApp, 28.6% used Instagram, and 14.3% used Facebook as platforms to commit cybercrimes. WhatsApp's higher usage suggests that cybercriminals find it convenient for carrying out their malicious activities.

(17) Response on Whether the Accused was Known or Unknown: The majority (78.6%) of victims reported that the person committing the crime was unknown to them. However, 21.4% mentioned that they knew the perpetrator. This highlights the involvement of both known and unknown individuals in cybercrimes.

(18) If Known, Whether the Accused was Known or Unknown: Out of the participants who knew the accused, 40% were from the workplace, 30% from the neighbourhood, 20% from the family, and 10% from the friend circle. These findings indicate that not only unknown individuals but also acquaintances and close relations can be involved in cybercrimes.

(19) If the Person Belongs to Work Place or Business, He was Your: Among the participants who knew the accused from the workplace or business, 78% identified the accused as their boss. This suggests that individuals in higher positions may misuse their authority to harass their subordinates using social media platforms.

(20) If He was Close, Whether the Person was Known: Among participants who knew the accused and were close to them, 30% mentioned that the accused was a relative, 10% said the accused was their own husband, and 60% belonged to another category. This finding underscores the fact that close relations and significant others may also resort to cybercrimes.

(21) Response on Steps Taken by the Females after Being Victim of Cybercrime: Among the female participants, 35.7% chose to block the perpetrator, while an equal percentage (35.7%) blocked the person and lodged a complaint with the cybercrime department. Additionally, 14.3% informed their parents about the incident, and 7.1% took no action. These responses demonstrate that a significant number of participants took proactive steps to address the cybercrime, such as blocking the perpetrator and reporting the incident to relevant authorities. Informing parents also reflects the victims' concern about their family's well-being and their image in society.

(22) Response on Not Taking Any Step against the Accused: Among the female participants, 33.3% did not take any action against the accused because they were not mentally prepared to launch a complaint, and an equal percentage (33.3%) chose to neglect or cover up the act if the harasser was close to them. An additional 22.2% did not file a complaint due to family constraints, fear of notoriety in society, or a lack of belief in the efficacy of the cybercrime department. It is concerning that some victims did not take action due to psychological reasons, fear of repercussions, or a lack of faith in the system.

(23) Response on the Consequence of Such Crime on Mental Health: The data showed that 30% of female participants experienced emotional stress like shock, helplessness, and trauma, while another 30% reported emotional trauma, including feelings of anger, fear, sadness, and nightmares. Moreover, 40% felt insecure and always stressed, fearing someone was following them. These responses highlight the severe impact cybercrimes can have on victims' mental health, leading to emotional distress, anxiety, and a sense of insecurity.

(24) Response on the Consequence of Such Crime on Their Family: Among the female participants, 54.5% mentioned that there was no effect on their family, but 36.4% stated that their family members also suffered mental agony as a result of the defamation caused to the victim. Additionally, 9.1% reported their family experiencing financial consequences due to the cybercrime. This emphasizes that cybercrimes do not only affect the victim but also have a ripple effect on their family members' mental well-being and financial stability.

(25) Response on the Consequence of Such Crime on Social Status: The data revealed that 45.5% of participants felt socially insecure, and an equal percentage felt socially isolated, while 9.1% reported no effect on their social image. These responses indicate that cybercrimes can negatively impact victims' social standing, causing feelings of insecurity and isolation in their social circles.

(26) Response on the Consequence of Such Crime in Their Life: Among the female participants, 18.2% had to stop their education or change their institute, 9.1% experienced relationship losses, while the majority (72.7%) reported that their life was not affected. These findings underscore the potential long-term consequences of cybercrimes, such as disrupting education and personal relationships, particularly for young victims.

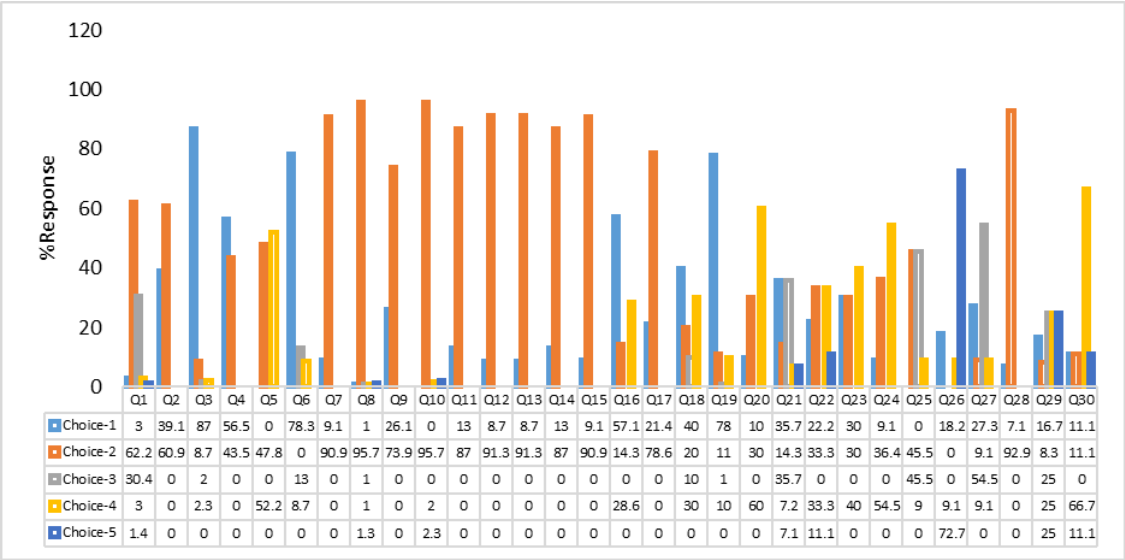
(27) Response on Acts Done After Being a Victim of Such Crime: According to the data, 27.3% of female participants stopped using social media, 9.1% continued using social media but could not trust anyone on digital platforms, and 54.5% used social media cautiously. These responses highlight the impact of cybercrimes on victims' digital behaviour, as many became more cautious and mistrustful on social media platforms.

(28) Response on Suicidal Thoughts Due to Harassment on Social Media: Out of the female participants, 7.1% revealed that they had attempted suicide after being a victim of cybercrime. This alarming finding underscores the severity of the mental trauma experienced by some victims, leading them to resort to extreme measures.

(29) Response on Current Thoughts After Being a Victim of Cybercrime: Among the female participants, 16.7% lost trust in social media, 8.3% believed that social media made them vulnerable to cybercrime, 25% felt that media was not trustworthy and kept information unsafe, and another 25% thought that social media remained trustworthy and kept information safe. These responses indicate the mixed perceptions and attitudes of victims towards social media platforms after experiencing cybercrimes.

(30) Response on How Victims Recovered from Mental Agony: According to the data, 11.1% of female participants sought medical help, an equal percentage sought spiritual help, and 66.7% took self-efforts to forget the crime and move on. The fact that most victims relied on self-efforts to cope with the mental agony highlights the need for mental health support and counseling services for cybercrime victims.

(31) Response on Safety Regarding the Use of Social Media: Among the female participants, 68.2% felt that digital platforms were still safe, while 31.8% believed they were no longer safe. These responses underscore the need for enhanced safety measures on social media platforms and increased awareness about digital security. All the responses have been shown in Fig. 4.



	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	Q15	Q16	Q17	Q18	Q19	Q20	Q21	Q22	Q23	Q24	Q25	Q26	Q27	Q28	Q29	Q30
Choice-1	3	39.1	87	56.5	0	78.3	9.1	1	26.1	0	13	8.7	8.7	13	9.1	57.1	21.4	40	78	10	35.7	22.2	30	9.1	0	18.2	27.3	7.1	16.7	11.1
Choice-2	62.2	60.9	8.7	43.5	47.8	0	90.9	95.7	73.9	95.7	87	91.3	91.3	87	90.9	14.3	78.6	20	11	30	14.3	33.3	30	36.4	45.5	0	9.1	92.9	8.3	11.1
Choice-3	30.4	0	2	0	0	13	0	1	0	0	0	0	0	0	0	0	0	10	1	0	35.7	0	0	0	45.5	0	54.5	0	25	0
Choice-4	3	0	2.3	0	52.2	8.7	0	1	0	2	0	0	0	0	0	28.6	0	30	10	60	7.2	33.3	40	54.5	9	9.1	9.1	0	25	66.7
Choice-5	1.4	0	0	0	0	0	0	1.3	0	2.3	0	0	0	0	0	0	0	0	0	0	7.1	11.1	0	0	0	72.7	0	0	25	11.1

Figure 4: Comparative study of responses received.

5.2. Cyber Crime Investigation Cases

(1) Cases Reported during January 2021 to December 2021: In the given period, a total of 100 cybercrime cases committed by youngsters between the ages of 15 and 35 were reported. Out of these cases, 59% were from rural areas,

while 14% were from urban areas. This data suggests a concerning trend of increasing cyber criminality in rural areas, indicating the need for targeted awareness and preventive measures in these regions.

(2) Complaints Lodged by Victims: Regarding cybercrimes committed by male youngsters, 7 complaints were lodged from urban areas, and 11 complaints were lodged from rural areas. The data highlights that girls from rural areas are proactive in lodging complaints, signaling a growing awareness of cybercrimes and the importance of seeking justice. This indicates a positive step towards empowering victims and holding perpetrators accountable.

(3) Age of Accused: The data reveals that all the cybercrimes were committed by male youngsters in the age group of 15 to 35 years. Among them, 75% (6 youngsters) of the accused were from rural areas, while 25% (2 youngsters) were from urban areas. This suggests that youngsters from rural regions are more involved in cyber criminal activities compared to their urban counterparts. Possible reasons for this disparity could be higher unemployment rates or a lack of awareness about the consequences of engaging in cybercrimes.

(4) Conviction Rate: Surprisingly, during the studied period, no accused in the reported cybercrime cases were convicted. This points towards potential challenges in the investigation and prosecution of cybercrimes. Enhancing the technical capabilities of law enforcement agencies and ensuring specialized cybercrime investigation units can contribute to improving the conviction rate and deterring future cybercriminals.

(5) Compensation to Victims: The data indicates that either no victims applied for compensation, or none of them received compensation from state government schemes designed to support victims, such as the Manodhairya Scheme for Rape victims, Children who are victims of Sexual Offences and Acid Attack Victims (Women and Children), and Maharashtra victim compensation scheme. These schemes aim to provide financial assistance and support to victims, but their underutilization could be attributed to a lack of awareness among victims or procedural challenges in accessing compensation.

INTERPRETATION BY PARETO ANALYSIS:

The data on cyber crimes by youngsters against girls and women reported from January 2021 to December 2021 was analyzed using the Pareto principle, also known as the 80/20 rule. The Pareto principle suggests that roughly 80% of the effects come from 20% of the causes. Let's apply this principle to the provided information. Pareto analysis reveals that cybercrime predominantly affects young individuals, especially those aged 21-25 years, residing in urban areas. WhatsApp is the primary platform used by perpetrators, and cyberstalking is a common crime faced by victims. While a significant proportion of the accused remain unknown, known perpetrators are often associated with workplaces or living areas. The consequences of cybercrime on mental health and social well-being are substantial. Additionally, the analysis of reported cases highlights the need for improved conviction rates and victim support mechanisms. Rural vs. Urban Cases: Out of the 1000 reported cyber crime cases, 59% were from rural areas, and 49% were from urban areas. This indicates that a higher proportion of cyber crimes are occurring in rural areas, contributing to 80% of the total cases. Therefore, rural areas account for the majority of cyber criminality (Fig. 5).

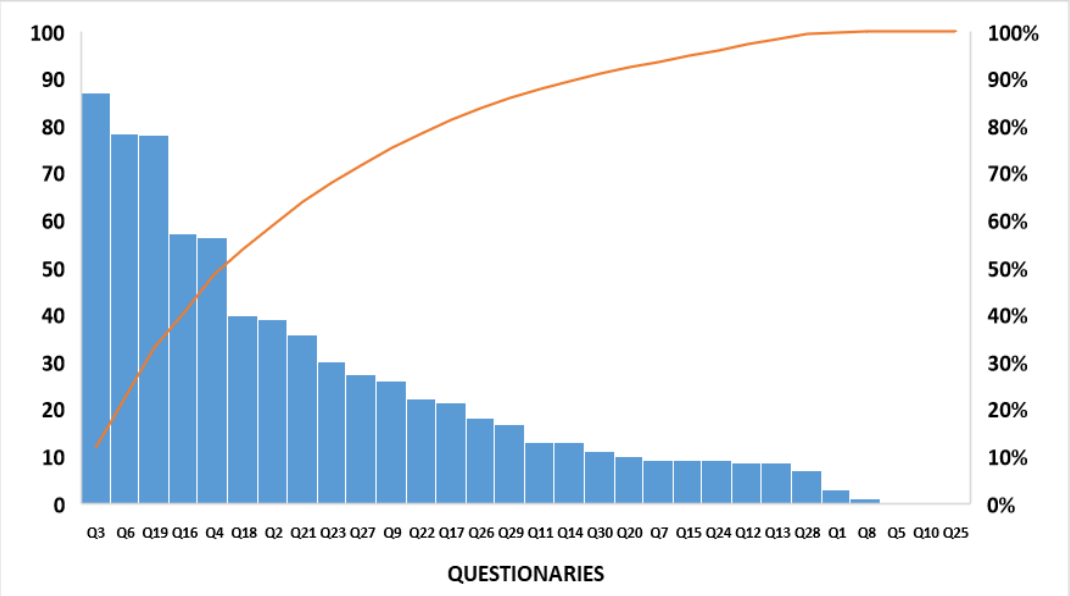


Figure 5: Pareto chart for the analysis cybercrimes on the basis of responses.

In case of data received from cyber cells, among the reported cases, 700 complaints were lodged from urban areas, and 1100 complaints were lodged from rural areas. These complaints represent the actions taken against the cyber crimes, and they constitute approximately 18% of the total cases. Thus, around 20% of the cases have resulted in formal complaints. Accused Distribution: All the accused perpetrators were male youngsters. Among them, 75% were from rural areas, while 25% were from urban areas. This means that rural youngsters account for 80% of the accused in cyber crimes. 80% of cyber crimes are happening in rural areas, indicating a higher prevalence of cyber criminality in rural regions. Approximately 20% of the reported cases have resulted in formal complaints, suggesting that only a small portion of the victims took legal action. Rural youngsters constitute 80% of the accused, indicating a higher involvement of rural youth in cyber criminal activities compared to their urban counterparts (Fig. 5). The analysis highlights the need for increased awareness and preventive measures to address cyber crime in rural areas and to encourage victims to report such incidents to the authorities. Additionally, measures to educate youngsters, especially in rural regions, about the consequences of cyber crimes and the importance of cyber ethics may help reduce the overall occurrence of such offenses.

6. FINDINGS :

Findings from the survey reveal a range of concerns and potential vulnerabilities.

(1) Crimes faced by girls and women: 78.3% of victims used WhatsApp on Android phones, indicating its prevalence in cybercrimes. 56.5% of college girls experienced cybercrimes, including hacking, stalking, sexting, and harassment. In 78.6% of cases, criminals were known to the victims and often from their workplaces. After the incidents, 35.7% of girls blocked the accused and filed complaints, while 7.1% took no action. Surprisingly, 11.1% of girls lacked belief in the effectiveness of the cybercrime department.

(2) Consequences in victims' life: 36.4% experienced emotional stress and mental agony, including shock, helplessness, trauma, anger, fear, and sadness. 7.1% attempted suicide due to cybercrime, and 45.5% felt socially isolated. 72.7% reported no effect on their routine life, while 18.2% had to halt education or change institutes.

(3) Consequences in victims' life: All cyber criminals targeting girls and women were young males. 59% of cases were from rural areas, and 49% were from urban areas. 75% of the accused were from rural areas, and no one was convicted during the study. Victims did not receive compensation from government schemes.

7. SUGGESTIONS:

Contact the nearest cyber cell or police station if you are a victim of cybercrime. File complaints anonymously through the National Cyber Crime Reporting Portal. If your data is compromised, keep copies of the original and compromised data. Preserve evidence in cases of email misuse, such as extracting email extension headers and saving offending emails to your computer's hard drive.

8. RECOMMENDATIONS:

Increase cyber security awareness. Avoid responding to irrelevant/fraudulent messages. Never share personal information in email replies. Be cautious of fraudulent websites. Follow data protection guidelines. Use strong, secure passwords and update them regularly.

9. REMEDIAL MEASURES:

Digital Literacy Conduct digital literacy campaigns to educate women on cybersecurity. Strengthen reporting mechanisms for easy and confidential reporting of cybercrimes. Establish a robust legal framework and support cells to handle cybercrimes involving women.

10. CONCLUSION:

The research demonstrates the application of the Pareto principle to identify the most common cybercrimes faced by women during the COVID-19 pandemic in Maharashtra. During the COVID-19 situation, data analysis revealed a significant increase in cyber crimes against women (Lassies) who were studying or working outside their homes, with workplaces being the primary target. Encouragingly, women from rural areas showed increased awareness by filing complaints. Furthermore, combating cybercrimes requires a multi-pronged approach involving awareness, education, capacity-building for law enforcement, and improved support mechanisms for victims. By addressing these issues collectively, society can strive towards creating a safer digital environment and protecting individuals from cyber threats and exploitation.

Conflict of interest:

The authors declare no conflicts of interest.

REFERENCES:

1. Cox L, Alfredsson E, Psouni E. Coparent exclusion, prenatal experiences, and mental health during COVID-19 in Sweden. J Fam Psychol. 2023 Jul 20.
2. Refaeli T, Schuman-Harel N, Brady E, Mann-Feder VR, Munro ER, van Breda AD. Widening the care gap? An international comparison of care leaving in the time of COVID-19. Am J Orthopsychiatry. 2023 Jul 20.
3. Hawdon J, Parti K, Dearden TE. Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. Am J Crim Justice. 2020;45(4):546-562.
4. Hoheisel R, van Capelleveen G, Sarmah DK, Junger M. The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. Comput Secur. 2023; 128:103158.
5. Lallie HS, Shepherd LA, Nurse JRC, Erola A, Epiphaniou G, Maple C, Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Comput Secur. 2021 Jun;105:102248.
6. Modecki KL, Minchin J, Harbaugh AG, Guerra NG, Runions KC. Bullying prevalence across contexts: a meta-analysis measuring cyber and traditional bullying. J Adolesc Health. 2014 Nov;55(5):602-11.
7. Gilbert M, Fernet M, Hébert M, Couture S. Diversity of Profiles and Coping Among Adolescent Girl Victims of Sexual Dating Violence. J Child Sex Abus. 2023 Jul-Dec;32(5):596-614.
8. Casey E, Barnum S, Griffith R, Snyder J, van Beek H, Nelson A. Advancing Coordinated Cyber-investigations and Tool Interoperability using a Community Developed Specification Language. Digit Investig. 2017;22: 10.1016/j.diin.2017.08.002.
9. Veena K, Meena K, Kuppusamy R, Teekaraman Y, Angadi RV, Thelkar AR. Cybercrime: Identification and Prediction Using Machine Learning Techniques. Comput Intell Neurosci. 2022 Aug 27; 2022:8237421.
10. https://en.wikipedia.org/wiki/Maharashtra
11. Lahane T. COVID-19: The battle of Maharashtra. Indian J Ophthalmol. 2021 Mar;69(3):477-478.
12. Harvey HB, Sotardi ST. The Pareto Principle. J Am Coll Radiol. 2