Competitive Social Sciences Research Journal (CSSRJ), 2 (3), 34-51
ISSN(Print):2708-9029,ISSN(Online):2708-9037
www.cssrjournal.com

Cybercrimes against Women in Pakistan: Feminist Narratives of Resistance, Resilience & Coping Strategies

***Maliha Gull Tarar**
Department of Social Work, University of Sargodha, Pakistan

Aaqib Shahzad Alvi
Department of Social Work, University of Sargodha, Pakistan

Yasir Aleem
College of Law, University of Sargodha

Abida Bajwa
Department of Social Work, University of Sargodha, Pakistan

*Email of the corresponding author: maliha.gul@uos.edu.pk

ABSTRACT

The study was conducted to understand the nature of cybercrimes against women and their resistance, resilience and coping strategies. To have in-depth analysis of cybercrime related women's narratives, qualitative research methodology was used to conduct this research and the research data was collected from Lahore, Faisalabad, Multan, Gujranwala and Rawalpindi, where Federal Investigation Authority's cybercrime wings were already working. Total 41 women were interviewed and the number of interviews was based upon saturation of data. The research concluded that ineffective state response, identity crisis of state institutions, women's unique geographic location and cultural notion of honor restricted women's access to their legal rights. However, women were resistant and resilient against cybercrimes but the level of their resistance and resilience was directly linked to their social status and cultural association. Furthermore, women were having unique coping strategies influenced by their financial status, family education, legal awareness and family support level. Majority of the women were using normalization, gender concealment and withdrawal as coping strategies against cybercrimes.

Keywords: FIA, Feminist discourse, Honor Culture, Violence.

Tarar, M.G., Alvi, A.S.. Aleem, Y.&Bajwa, A. (2021). Cybercrimes against Women in Pakistan: Feminist Narratives of Resistance, Resilience & Coping Strategies. Competitive Social Sciences Research Journal (CSSRJ), 2 (3), 34-51.

INTRODUCTION

Cybercrime is a global social issue that affects people everywhere. Increased dependency on the internet and expansion of information and communication technologies (ICT) has resulted in an unprecedented increase in cyber attacks. In last two decades, the possible risks of virus attacks, online hacking, information security breaches and other cybercrimes have rapidly increased and cybercrime has surfaced as a growing concern for individuals and various organizations' information security policies as well as the most important area of investigation for criminologists. Cybercrime refers to illegal activities carried out by criminals using the internet and other digital technologies (Böhme & Moore, 2012; Wada & Odulaja, 2012; Arachchilage & Love, 2014). As cybercrime is a criminal act that involves the use of computing devices or other forms of information and communication technologies (ICT) but there is no precise definition of cybercrime because different researchers and agencies defined it differently depending on their location and state. It is also known as computer crime, internet crime, and high-tech crime (Brenner & Goodman, 2002; Kowalski, 2002).

Cybercrime refers to a wide range of criminal activities involving the illegal use of information and communication technologies (ICT). The term "cybercrime" is used interchangeably by academics, governments and law enforcement agencies to describe online criminal activities such as attacks, unauthorized access to user's confidential data. Virus attacks, intellectual property theft, phishing, hacking, virus distribution, online fraud and misdirection of communications, system interruption or intervention, money laundering, and hacking are just a few examples of cybercrimes (Kraemer-Mbula et al., 2013; Hunton, 2009; Malik & Islam, 2019).

In today's world, there are numerous types of cybercrime. According to research and investigations, the types of crime that occur in every part of the world have yet to be explored. Identity fraud is a type of cybercrime fraud and is defined as the acquisition of money, services, goods, or other benefits through the use of a false identity. Moreover, international community splits cybercrime into nine basic categories while developing anti-cybercrime legislation. Among the categories are intellectual property infringement, criminal/procedural legislation, privacy protection, internet economic crime, forgery, internet fraud, illegal access, teen pornography and illegal/harmful content (Blindell, 2006; Hamad, Manan, Shabiralyani, & Iqbal, 2015).

Pakistan is one of the countries that have passed cyber legislation to protect and promote electronic transactions. It shows that the laws intended to shield the cyber community from intentional crimes are insufficient to protect non-commercial issues, particularly the use of the internet to spread extremist ideologies. Extremists are also engaged in illegal activities on social media platforms around the world, particularly in Pakistan (Ullah, Amir, Khan, Asmat, & Habib, 2015).

To address cybercrime issues, Pakistan established a National Response Center for Cyber Crimes (NR3C) under the Federal Investigation Agency (FIA). NR3C has a wide range of responsibilities as it is dynamically involved in detecting and resolving frauds, financial embezzlements and malpractices that occur in the virtual environment. Additionally, it is to provide security education and training to private and government organizations. In order to carry out its task, NR3C maintains cooperation with various international organizations to collaborate and make joint efforts in this regard because combating cybercrime necessitates a multifaceted approach involving all communities (Riaz, & Riaz, 2015; FIA, 2020).

Women in Pakistan are subjected to a high level of cybercrimes. In 2018, 65 percent of cybercrimes were committed on Facebook, including blackmailing and harassment of women. However, the vast majority of such cases went unreported and unregistered for a variety of reasons including a fear of losing one's dignity and a lack of awareness (Qureshi, Abbasi, & Shahzad, 2020). The data also indicated that cybercrime complaints predominantly increased over the last three years. The Cyber Crime Wing received complaints about financial fraud, harassment, hacking and fake profiles. Other types of cybercrime were blackmailing, threats, stalking, blasphemous content, spamming, pornography, child pornography, spoofing, identity theft, and so on. Moreover, Facebook, WhatsApp, Instagram, Twitter, Snapchat, TikTok, and other social media platforms were also used for cybercrimes (FIA, 2020; Hayder, 2020).

LITERATURE REVIEW

Literature suggests that three most important types of cybercrimes are cybercrime against individuals, cybercrime against organizations and property, and cybercrime against the government. Individual cybercrime is defined as the cybercrime that has an effect on a person or his/her possessions directly. It is also a type of cybercrime in which someone spreads hateful or illegitimate information via internet. Pornographic distribution, cyber stalking and human trafficking are all examples of this (Donalds, & Osei-Bryson, 2019). In addition, the number of internet users in Pakistan is rapidly growing. This rapid adoption of digital technology, combined with a general lack of cyber security consciousness among Pakistani population, has created a productive position for cyber criminals to exploit the digital medium and individuals (Munir, & Gondal, 2017; Zahoor, & Razi, 2020).

Qarar (2018) reported that Pakistan suffers more from cybercrime and other malevolent acts such as impersonation, blackmail, fake news/defamation, and unauthorized data usage than from traditional forms of cybercrime such as digital theft, fraud, and so on. In Pakistan, the legislation to combat cybercrime is rather primitive. The Federal Investigation Agency (FIA) is currently the legal body in charge of dealing with cybercrime. It was reported that in 2017, it received only 1290 inquiries but this number is very low because the majority of the population is unaware of how to report cybercrimes, and a public education campaign is also required (Shahid, Kauser, & Zulqarnain, 2018).

Digital Rights Foundation (2017) reported that there were numerous different motives behind cyberspace violence and women were repeatedly major target of it. Aslam (2017)

also highlighted that cybercrime in Pakistan has increased at an alarming rate due to an increase in the number of social media users and apparent ignorance on the part of parents in terms of teaching and guidance. The majority of social media users lack knowledge and guidance from their elders, peer groups, friends, and others on how to engage in online activities while maintaining personal safety and security and avoiding harm to other users. Furthermore, Haq & Atta, (2019) reported that in order to effectively combat online harassment, society must participate in discouraging offenders and avoiding stereotypes that make it difficult for victims to report incidents. Adoption of upcoming advances in ICT can make it hard for the offender to conceal their identity. Moreover, cybercrime can affect both individuals and organizations. Attackers frequently target organizations for direct financial gain or to threaten or disrupt specific actions. Cybercriminals typically target organizations, whereas individuals are more likely to become victims of non-specific, broad attacks such as cold-calling scams or phishing emails.

According to Federal Investigation Agency's data, the majority of Pakistan's cybercrime cases were occurring in Karachi. Every day, Karachi's cyber wing received nearly 20 cybercrime complaints. In the year 2018, nearly 5500 cases of cybercrime were reported in Lahore. These cases included harassment, blackmail, stalking, invasion of privacy, impersonation, and fraud, among other things (Qarar, 2018; FIA, 2020).

Qureshi, Abbasi, & Shahzad (2020) conducted a study about cybercrimes and indicated that women victims were mostly educated and between the ages of 21 and 30. The most common forms of cyber harassment were the posting of images and videos on various online forums. The most common means of harassment were cell phones and Facebook. The main intend of harassment was money demands and physical meetings. They also highlighted that despite the fact that it is difficult to avoid online harassment, we can reduce it to a greater extent. Individuals, law enforcement agencies, and the government must all collaborate to achieve this because prevention can better address the issue. Raising public awareness about cyber bullying is the most effective way to prevent it. No law enforcement entails providing a podium for cyber criminals to commit online harassment offences. If the law is guaranteed to be followed, it can be very helpful in reducing cybercrimes.

In Pakistan, the Prevention of Electronic Crimes Act (PECA) was passed in August 2016 which was an analysis from common society and advanced rights associations. The flawless worded nature of the law matter that it could, and eventually was utilized to quiet resistance and brace down on free discourse. The Federal Investigation Agency's Cybercrime Wing (CCW) is governed by laws enacted under the Prevention of Electronic Crimes Act (PECA) 2016, which addresses the growing threat of cybercrime. This crime fighting unit was formed to detect and combat the incidents of technological exploitation in society. It is the only one of its kind in Pakistan, receiving complaints directly and taking legal action against cyber criminals (Shahid, Kauser, & Zulqarnain, 2018; Digital Right Foundation, 2017; FIA, 2020).

Literature also highlighted that there are a few issues with the current enactment, its execution and the foundations entrusted with the execution make a few hindrances for women and other victims of online viciousness. The Federal Investigation Agency's (FIA) National Response Center for Cyber Crime (NR3C) has the authority to conduct internal investigations under PECA. The NR3C is severely understaffed and under-resourced, making it unable to manage the current crisis effectively. The NR3C's offices are only

located in major cities throughout Pakistan (Quetta, Peshawar, Lahore, Karachi, Rawalpindi and Islamabad). The absence of geological association of these workplaces is a genuine worry, as it implies that women living outside these selected urban communities should leave their region of habitation to just record a dispute; which has the consequence especially for disadvantaging women in far away areas (Shahid, Kauser, & Zulqarnain, 2018).In 2017, Aslam also highlighted that the NR3C workplaces were criminally understaffed and exemplified that the Lahore office was having only 13 specialists (field officials), including two associate chiefs, four investigators, and five Sub-Inspectors. The Deputy Director of the Lahore branch admitted that those13 men covered regional wards within Punjab's 32 regions with just a single accessible authority vehicle.

Bakhsh, Mahmood and Awan, (2016) analyzed cybercrimes and cyber laws in relation to Gulf countries and Pakistan and reported that cyber laws have been developed in almost every developing and developed country, but the implementation was lacking, particularly in the Middle East and Southeast Asia due to widespread legal illiteracy.

Citron (2015) indicated that cybercrime victims' lives were fundamentally altered. They left because they did not feel safe at home, and they frequently switched names. Victims were experiencing intense emotional distress, anxiety, and depression. Importantly, online attacks can discourage people from participating in and communicating online. Victims had their blogs, social media profiles, and websites disabled. They withdraw because staying online frequently exacerbates the situation. Citron (2015) also reported the cybercrime situation in the USA that the victims were frequently advised to ignore the abuse. Many state's harassment and stalking laws only cover abuse sent directly to the victims; they do not cover content posted on third-party sites, so legislators still have a lot of work to do. Women can report defamation, public disclosure of private information, and intentional infliction of emotional distress but financing these claims is difficult. A private lawsuit is extremely expensive, and most victims cannot afford to hire an attorney. Even more difficult is convincing an attorney to take a case on contingency.

Rehman (2020) highlighted that academics and researchers play an important role in educating the general public about cybercrimes phenomena and how to deal with them. As cybercriminals have developed more advanced strategies to expand their criminal enterprise, society must provide much more knowledge and education about how to combat these threats and cyber attacks, which are causing tremendous pain, anguish, discomfort, and billions of dollars in damages to many people and organizations around the world.

RESEARCH METHODOLOGY

Considering the nature of the study, qualitative research methodology was used to conduct this research. Qualitative research methodology was very helpful to have in-depth analysis of women's narratives of resistance, resilience and coping strategies against cybercrimes. An interview guide was developed to conduct in-depth interviews of women respondents. The research data was collected from Lahore, Faisalabad, Multan, Gujranwala and Rawalpindi, where Federal Investigation Authority's cybercrime wings were already working. Inclusion criteria were based upon women's cyberspace existence, experiences

and understanding about cyber crimes. Total 41 women were interviewed and the number of interviews was based upon saturation of data.

RESULTS AND DISCUSSION

Respondent's Demographic Profile

Tables below present participants' demographics.
Table 1: Details about the location, number and in-depth interviews

Sr. No	Interview Locations	No. of In-depth Interviews
1	Lahore	**10**
2	Faisalabad	**07**
3	Multan	**08**
4	Gujranwala	**07**
5	Rawalpindi	**09**
Total		**41**

This table shows that the data was collected from Lahore, Faisalabad, Multan, Gujranwala and Rawalpindi, where Federal Investigation Authority's cybercrime wings were already working. Total number of participants was 41 and 10 participants were interviewed from Lahore, 07 from Faisalabad, 08 from Multan, 07 from Gujranwala and 09 were from Rawalpindi.

In Pakistan, the Cybercrime Wing is divided into six operational zones and fifteen Cybercrime Reporting Centers (CCRCs). Under the overall supervision of Director General FIA, the Cybercrime Wing is led by an Additional Director General (ADG), who is assisted by Directors Administration and Operations (FIA, 2020).

Table 2: Respondent's Age

Sr. No	Age	Frequency
1	21-25	**10**
2	26-30	**12**
3	31-35	**11**
4	36-40	**06**
5	41-45	**02**
Total		**41**

The research data indicated that 10 respondents were 21-25 years old, 12 were 26-30 years old, 11 were 31-35 years old, 06 were 36-40 years old while 02 were 41-45 years old.

Table 3: Educational Status

Sr. No	Educational status	Frequency
1	Literates	**41**
Total		**41**

All the respondents were literate and they were able to access internet and social media platforms.

Table 4: Respondent's Residential Background

Sr. No	Residential Area	Frequency
1	Rural	**19**
2	Urban	**22**
Total		**41**

In the research study urban and rural women shared their experiences and 19 participants were from rural areas while 22 were from urban areas.

Table 5: Respondent's Family System

Sr. NO	Family System	Frequency
1	Joint	**18**
2	Nuclear	**23**
Total		**41**

Majority of the respondents, 23 were from nuclear family system and 18 were from joint family system.

Table: 6. Respondent's Marital Status

Sr. No	Marital Status	Frequency
1	Unmarried	**11**
2	Married	**24**
3	Widows	**03**
4	Divorced	**03**
Total		**41**

This table provides detail about respondent's marital status. According to this table, 11 research respondents were unmarried, 24 were married, 03 were widows and 03research participants were divorced.

Table 7. Respondent's Economic Class

Sr. No.	Economic Class	Frequency
1	Low Income class	**03**
2	Middle class	**34**
3	Higher Class	**04**
Total		**41**

This table shows that majority of the respondents, 34 were from middle class and 04 were from higher class. There were only 03 respondents from lower income class.

FEMINIST NARRATIVES OF RESISTANCE, RESILIENCE & COPING STRATEGIES

A married respondent (age 30 years) shared,

> *"My Facebook account was hacked and the hacker used my contacts and pictures to harass me. For many days, I was unable to share it with my family as they were against women's use of Facebook, especially against uploading pictures but the hacker himself sent vulgar massages to my family members. Complaining to law enforcement agencies was not an option for us as my father said, it*

is enough to face disrespect…. contacting the police means inviting more troubles….so be silent and there is no need to expose more".

A respondent from rural area (unmarried, age 24) shared,

"I was having a Facebook account and came to know that someone made an account with my name and bio data. That fake account was having 1542 male friends including many from my neighborhood. That was a worst surprise for me and my family because everyone was considering that as my account. I faced really tough time because of that as my own family was very angry and upset. It was disrespectful and shameful for my family that their daughter was having many male friends. My family's thorough investigation explored that one of my female class fellow did all that just to defame me. Women are considered honor of a family and complaining lodging a complaint about that sensitive issue was even more shameful for my family".

Literature also supports that women are the most vulnerable to cyber bullying. Victimization is more common among single women, young adults, and employed students. Women's increased victimization may be attributed to their frequent use of social media. Time spent online and lack of knowledge about cyber security measures is associated with digital victimization (Anjum, 2020).

Previous studies reported that cyber stalking is a cybercrime against women that involves monitoring a person's activities through internet, identifying the victim's social group and frequent interactions, sending a message and email to the victim or any fellow victims with violent threats, contents or personally attacking the victim and to mount fear. Generally, the majority of cyber-stalking victims are women and men are perpetrators (Cavezza, & McEwan, 2014; Prameswari, 2017). Moreover, Agarwal and Kasuhik (2014) reported that morphing is the illegal or false identity editing of an original image or photo. Pictures of one or more women downloaded by the criminal are then uploaded/reinstalled on a different website using a forged profile.

An unmarried respondent (age 23) shared,

"I was in love with my class fellow….he was decent or I was considering him a reasonable person just because I loved him so much. We shared pictures, messages and even our cyber profiles. We planned to get married after completing our studies but he started ignoring me after leaving the educational institution. I reminded his promise of getting married again and again but he was not giving any reasonable/satisfactory response…..After some months…..I came to know that he was making fun of my feelings in different WhatsApp and Facebook groups. He also shared my pictures in those groups to show off that I am crazy for him……that was a shock for me which destroyed my personality, confidence, self-esteem and everything. I was angry and heartbroken so asked

him aggressively but he blackmailed that he would share all intimate content at internet. I was unable to inform my family and friends to avoid further consequences. I was unable to report concerned law enforcement agencies to protect my family's honor……it was all my mistake……my bad judgment…..my blind trust…..but cyberspace is making our life more vulnerable. No one needs any type of permission to upload any content and people are using internet related forums to harass, exploit and perpetrate violence against women".

Halder and Jaishankar (2012) recognized online defamation as a cybercrime against women and explained that it involves publication of fake information through internet about an individual to harm the target person's repute.

Previous studies also highlighted the effects of cybercrimes against women are mental, social, physical and monetary. The most widely recognized effects are mental effect, which are widely experienced by women who experience digital viciousness. Many women victims of cybercrimes experienced mental health consequences PTSD, sleep disorders, understanding of gigantic dread that shielded them from going out, sentiments of outrage, being determined to have PTSD, self-destructive contemplations and endeavored self destruction (West, 2014).

A divorced respondent (age 38) shared personal experiences that ex-husband uploaded her private and intimate images at Facebook and YouTube. She said,

"It was a horrible time for me and my family……we were unable to share it with anyone……even to get help……our gender script is so different for women that if women face something they cannot even access their legal rights…….I tried to convince my family to get help in this but they thought it more insulting to complaint police……I asked a friend to help and accessed cyber crime wing's website…..we lodged a complaint but their interrogation was too slow and weird…..that was even more painful…..finally the family settled the issue …not the police and FIA".

Literature indicates that revenge pornography is an increasingly common subtype of cyber stalking /cyber harassment. It can be defined as the unauthorized online publication of clear videos or photographs of a person for the purpose of mortification. In intimate relationship issues, videos and photographs are frequently taken and voluntarily given to other individuals (Bennett, 2014; Franks, 2015). Literature also highlighted that although rancorous ex-intimates may engage in revenge pornography after a relationship has ended but this is not always the case. An unidentified hacker or stalker may illegitimately get access to a victim's intimate photographs and videos. As a result, some victims advocate the term "nonconsensual pornography" because as not all perpetrators are motivated by vengeance so the term "revenge pornography" can be misleading. Moreover, some people profit from the distribution of explicit content. Others are motivated by fame or entertainment. Furthermore, the victims of revenge pornography may suffer serious mental health consequences. The victims have to deal with long-term psychological and personal

consequences, as the widely disseminated photographs or videos may disturb them for the rest of their lives (Kamal & Newman, 2016).

A married respondent (age 37) shared,

> *"I am working in a public sector organization and it was mandatory for all the staff members to upload profile pictures at organization's website. Although many women colleagues were resistant to share their pictures yet we had to show resilience. After uploading the pictures, our profiles were public….. A few months later one of my colleague shared that there was a YouTube channel using our profile pictures for some indecent content and she sent link of that channel as well….when I opened that….It was a horrific experience for me. There was my official picture with title "divorcee looking for suitable match third time"…..it was so shameful…..that YouTube channel used my colleagues pictures and also of some women politicians…… I did nothing wrong but because of shame and guilt feelings, were unable to share with my husband and family…..I took five days to console myself and then met my other colleagues who were also the victims and then we decided to resist. We also discussed possible coping strategies and lodged complaints at FIA's cybercrime online portal. As educated women we were hoping to get their response but that is just a dummy portal and nothing happened even after lodging multiple complaints".*

Another victim of identity theft (age 40, widow) shared,

> *"That was so disrespectful……it was identity theft. In an honor based society a woman can live without food but not without honor…..we were resisting to share pictures at official site but no one considered our resistance so we had to show resilience to cope with autocratic, authoritative administrative policies of the organization. When a YouTube channel used my picture with inappropriate subtitles, some of our colleagues (men and women) were making fun of it. I reported to FIA cybercrime wing and YouTube as well but can you believe….that channel I still there even after three years of complaining and reporting. As a young widow, I am unable to follow lengthy legal procedures so I am silent and pretending to be normal*".

Lewis et al. (2015) published a study that claimed the frequency of online abuse reduced its impact; however, the data revealed that the frequency of abuse increased overall. This suggests that the effects of the "wallpaper of sexism" are cumulative and exacerbated rather than diluted by frequency. There is another parallel with the normalization thesis, in which survivors minimize their experiences because they are part of an ordinary routine of daily life.

Literature also indicates that not every victim of cyber bullying was having a public profile. The majority of victims were from ordinary backgrounds, such as teachers, nurses, dentists, and stay-at-home parents. The consequences for victims were severe. The professional fees for legal services were exorbitant. Moreover, the victims found it difficult to keep or obtain employment because abuse was prominently featured in online searches for their names (Citron (2015).

A respondent (age 45, divorced) shared:

> *"Establishment of complaint mechanism cannot change our honor culture….. If a woman becomes a victim of cybercrime she must has to face social stigma. It is direly needed to make people aware that cybercrimes are like other crimes and the state should address the complaints lodged at online portal as well".*

Another respondent (age 22, unmarried) shared,

> *"I used pseudonym for my social media profile to conceal my identity but someone made a fake Facebook account by using my identity and details. I reported Facebook many times but nothing happened so it is better to be silent".*

An unmarried respondent of urban area (age 28) shared that,

> *"Pakistani women are facing cyberspace violence but do not have necessary information to report concerned authorities….police culture is so corrupt and not women friendly so women have no option/ choice to contact law enforcement agencies. One of my friend filed complaint through FIA cybercrime wing but nothing happened".*

A married respondent (age 31) who was residing in urban area share,

> *"I was using Facebook and Instagram but immediately after my marriage, my friend's Facebook account got hacked and I received a message from her account with a link…..I just opened the link and that also hacked my account. I ignored that but within a few hours that hacker started blackmailing me. He sent inappropriate messages to my Facebook friends including my husband and mother-in-law. I cannot explain how much trauma I faced because of that…..I was newly married and unable to explain all that to my in-laws……No one was ready to listen me……no one was ready to accept that it was not because of me and my moral values…. That violent incident totally changed my family life as even in this age of technology, Pakistani women have some restrictions to get certificate of "a good woman". Moreover, contacting law enforcement agencies is even more difficult because of honor notion".*

Another respondent from rural areas (married, age 30 years) shared,

> *"I was having a social media account but closed that after my marriage as my husband don't like it. He thinks social media is not safe for women and people have negative opinion about women's internet use. I am totally agreed as I personally witnessed that even women do not like women's internet/ social media use. When I had an account, I also experienced that women are even more vulnerable in cyberspace as they can easily become a victim of identity theft, bullying and harassment".*

Another respondent (unmarried, age 21) stated,

> *"I was forced by my parents to delete all of my social media accounts after my Facebook account got hacked a few years ago. According to my parents, internet is not safe for women in Pakistan as we cannot even complaint anyone if have some issue. They also think that it is not morally appropriate for unmarried girls to have internet related accounts".*

An unmarried respondent of urban area (age 28) shared that,

> *"Pakistani women are facing cyberspace violence but do not have necessary information to report concerned authorities….police culture is so corrupt and nor women friendly so women have no option/ choice to contact law enforcement agencies".*

Literature also indicates that women can show their disappointment according to police responses because police deals every individual communication as a peculiar conduct, seizing the anguish resulted due to accretion of abuse. This depicts that the judiciary system has failed to counter more effectively the antisocial behavior and cybercrimes (Chakraborti, 2015).

Another respondent (married, age 35) from a middle class family shared that

> *"I faced cyber bulling on Facebook as someone made fake account with my name, bio data and picture. I reported Facebook many times but no action was taken. That person concealed my identity at internet and pretended as me. It made me upset and helpless but I was not able to do anything. I am married and unable to share it with my husband because I could not say anything about his reaction. I think Instagram offers better security than Facebook".*

According to secondary data, women are the victims of violence and discrimination based on gender and they are struggling for demanding their rights and status in society. Moreover, status of women is also affected with biological, socio-cultural and psychological course of actions (Cohen, 2002).

A respondent from rural background (married, age 28) shared,

> *"I have social media accounts but not with my real name as rural areas have more strict gender script for women so having social media accounts is not something to appreciate for rural women. Even those who have accounts cannot upload pictures and comments. If I cannot even share about having social media account, how can I share violence or bullying experience".*

A married respondent of urban area (age 32) shared that the government should take effective steps to help women who have been a victim of cyber violence and bullying and should capture the abuser as soon as possible.

A research respondent from rural location (Age 35, married) shared,

> *"Many rural women are very active at TikTok and Facebook but majority of them are using pseudonyms to conceal their identities. Pakistani rural women are even more resilient to report cybercrimes as they have limited access and social support because of cultural limitation and their unique geographic locations*".

Another research participant (age 37, married) shared,

> *"Pakistani society is stratified so women from each socio-economic class have different cyberspace/cybercrime experiences, resistance and resilience level. Furthermore, majority of them cannot even think to report a cybercrime experience because of their limited knowledge about the nature of cybercrimes and available resources to address the issue".*

The research participants highlighted that it is vital to makes women aware about cybercrimes and available legal options to deal with. Literature also indicated that computerized education trainings are imperative to lead change. It is additionally critical to build the mindfulness of women and young girls about the cybercrime laws, their security understanding while at the same time utilizing advanced media, utilization of cell phones and their privileges to expand their voice against brutality. Moreover, there is a great need to teach individuals about their own information wellbeing in cyberspace (Grant, Burke, & Van Heerden, 2015).

CONCLUSIONS

The study concluded that cybercrimes were affecting many Pakistani women but the victims were unable to access their legal rights to preserve family's honor and to avoid traditional police culture. Cyberspace did not need any validation or permission to share contents so women's privacy was badly suffered by that. Women victims of cybercrimes were feeling angry, annoyed and helpless. For some women, experience of cybercrime was more intense as compared to the bullying done in-person because the perpetrators were having advantage of hiding their identity behind the screens without the fear of punishment. The research also concluded that Pakistani women are considered custodian of family's

honor and majority of the women victims of cybercrimes preferred to keep their violence experience secret because of women's honor notion prevailing in the society. Women's resistance, resilience and coping strategies were influenced by multiple socio-economic factors. However, those who reported cybercrime experiences were not satisfied from the services provided by the state agencies. The study also concluded that the state is needed to challenge existing honor notions and to improve the quality of services for the welfare of women victims of cybercrimes.

RECOMMENDATIONS

- Women are victim of cyber violence and have limited awareness about state laws. It is needed to enact new laws and to enforce already existing policies. Moreover, awareness campaigns should be launched to introduce state policies and laws related to cyber bulling and violence.
- The state should introduce women friendly centers for victims of cyberspace violence and crimes. Moreover, psychiatric, psychological and social support should be provided to the victims.
- In Pakistan, family is considered a basic unit of support and women victims of violence also need support to complaint and address the issue. It is needed to sensitize the families that women victims of cybercrimes and violence also need family support.
- The state should evaluate the role and performance of state agencies dealing with cyber crimes and women's complaints.
- Financial support and advocacy services should be provided to women victims of cyber crimes to access legal rights and justice.

REFERENCES

Anjum, U. (2020). Cyber crime in Pakistan; detection and punishment mechanism. *Časopiso društvenom i tehnološkom razvoju*, *2*(2). Retrieved from https://www.ceeol .com/search/article -detail ?id=919062

Arachchilage, N.A.G. and Love, S. (2014), Security awareness of computer users: a phishing threat avoidance perspective, *Computers in Human Behavior, 38(1),* 304-312.

Aslam, S. (2017, October 23). Dealing with cyber crime needs more resources. *The News.* Retrieved from https://www.thenews.com.pk/print/238972%20-Dealing-withcyber-crime-needs more

Bakhsh, M., Mahmood, A., & Awan, I. I. (2016). A comparative analysis of cybercrime and cyberlaws in Islamic Republic of Pakistan, Kingdom of Saudi Arabia, and the United Arab Emirates. *Imam Journal of Applied Sciences*, *1*(1), 9-15.

Bennett, K. B. (2014). Revenge pornography: exploring tortious remedies in Texas. . *Mary's LJ*, *46*, 522-526

Blindell, J. (2006). Review of the legal status and rights of victims of identity theft in Australasia. Retrieved from http://www.acpr.gov.au./pdf/ACPR145_2.pdf

Böhme, R. and Moore, T. (2012), "*How do consumers react to cybercrime?*", eCrime Researchers Summit (eCrime), IEEE, pp. 1-12.

Brenner, S. W., & Goodman, M. D. (2002, December). *Cybercrime: The need to harmonize national penal and procedural laws*. In International Society for the Reform of Criminal Law 16th Annual Conference, Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice, December (pp. 6-10).

Cavezza, C., & McEwan, T. E. (2014). Cyberstalking versus off-line stalking in a forensic sample. *Psychology, Crime & Law, 20*(10), 955-970.

Chakraborti, N. (2015). *Hate crime: Concept, Policy, Future Directions*. New York, USA: Routledge.

Chiarini, A. (2013, November 19). I Was a Victim of Revenge Porn. I Don't Want Anyone Else to Face This. *The Guardian (U.S.),* Retrieved from https://www.theguardian.com/commentisfree/2013/nov/19/revenge-porn-victim-maryland-law change

Citron, D. K. (2015). Addressing cyber harassment: An overview of hate crimes in cyberspace. Case W. Res. *JL Tech. & Internet, 6,(*1). Retrieved from https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1076&context=jolti

Digital Rights Foundation (2017). *Online Violence Against Women in Pakistan: Submission to UNSR on Violence Against Women*. Retrieved from https://digitalrightsfoundation.pk/wp content/uploads/2017/12/UNSR-Submission-by-DRF.pdf

Donalds, C., & Osei-Bryson, K. M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*, 403-418.

Federal Investigation Authority, (2020), *Cyber Crime Wing*. Retrieved from https://fia.gov.pk/ccw#

Franks, M. A. (2015). *Drafting an Effective Revenge Porn' Law: A guide for Legislators*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468823

Grant, T., Burke, I., & Van Heerden, R. (2015). Comparing models of offensive cyber operations. *Leading Issues in Cyber Warfare and Security: Cyber Warfare and Security*, *2*, 35-52.

Halder, D., & Jaishankar, K. (2012). Legal Treatment of Cyber Crimes Against Women in USA. I*n Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 777-789). USA: IGI Global.

Halder, D., & Jaishankar, K. (2012). *Definition, typology and patterns of victimization. In Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1016-1042). USA: IGI Global.

Hamad, N., Manan, A., Shabiralyani, G., & Iqbal, N. (2015). A Quantitative Approach to Cybercrimes Impact on Society in Pakistan Case Study: Business Community of Southern Punjab. *Journal of Information Engineering and Applications, 5*(5), 50-55.

Haq, U., & Atta, Q. (2019). Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan. *International Journal of Computer Network & Information Security, 11*(1).

Hayder, H. (2020). *FIA's Cyber Crime Cell Registered 15,000 Cases in 2019*. Retrieved from https://propakistani.pk/2020/01/07/fias-cyber-crime-cell-registered-15000-cases-in-2019/

Hunton, P. (2009), The growing phenomenon of crime and the internet: a cybercrime execution and analysis model, *Computer Law and Security Review, 25*(6),528-535.

Kamal, M., & Newman, W. J. (2016). Revenge pornography: Mental health implications and related legislation. *Journal of the American Academy of Psychiatry and the Law Online, 44*(3), 359-367.

Kowalski, M. (2002). *Cyber-crime: issues, data sources, and feasibility of collecting police-reported statistics*. Canada: Canadian Centre for Justice Statistics.

Kraemer-Mbula, E., Tang, P. and Rush, H. (2013), "The cybercrime ecosystem: online innovation in the shadows?", *Technological Forecasting and Social Change, 80* (3),541 555.

Lewis, R., Rowe, M., & Wiper, C. (2017). Online abuse of feminists as an emerging form of violence against women and girls. *British Journal of Criminology, 57*(6), 1462-1481.

Malik, M. S., & Islam, U. (2019). Cybercrime: an emerging threat to the banking sector of Pakistan. *Journal of Financial Crime.* Retrieved from https://www.emerald.com/

Munir, A., & Gondal, M. T. (2017). Cyber Media and Vulnerability: A discourse on cyber laws and a probe on victimization of cybercrimes in Pakistan. *Global Media Journal: Pakistan Edition, 10*(2).

Prameswari, A. D. (2017). *Online Abuse Against Women in the Cyber Space as an Important Issue to Discuss.* Retreived from https://ascrim.ui.ac.id/wp content/uploads/sites/102/2018/11/Agustin-Dea-Prameswari.pdf

Qarar, S. (October 23, 2018) 'Cybercrime reports hit a record high in 2018: FIA' Dawn . Retrieved from https://www.dawn.com/news/1440854

Qureshi, S. F., Abbasi, M., & Shahzad, M. (2020). Cyber harassment and women of Pakistan: analysis of female victimization. *Journal of Business and Social Review in Emerging Economies, 6*(2), 503-510.

Rehman, T. U. (2020). International Cooperation and Legal Response to Cybercrime in Pakistan. *In Encyclopedia of Criminal Activities and the Deep Web* (pp. 424-434). USA:IGI Global.

Riaz, A., & Riaz, A. (2015, November). Causes and consequences of cybercrimes: An exploratory study of Pakistan. In 2015 First International Conference on Anti-Cybercrime (ICACC) (pp. 1-5). IEEE.

Shahid, K., Kauser, S., & Zulqarnain, W. (2018). Unveiling the evil; Pakistani young girls and online harassment. *Journal of Research and Reviews in Social Sciences Pakistan, 1*(2), 152-163.

Ullah, S., Amir, M., Khan, M., Asmat, H., & Habib, K. (2015, November). Pakistan and cyber crimes: Problems and preventions. In *2015 First International Conference on Anti-Cybercrime (ICACC)* (pp. 1-6). IEEE. Retrieved from https://ieeexplore.ieee.org/

Wada, F. and Odulaja, G.O. (2012), "Electronic banking and cyber crime in Nigeria-a theoretical policy perspective on causation", *African Journal of Computing &ICT, 4*(2), 69-82.

West, J. (2014). *Cyber-violence against women*. Vancour, BC: Battered Women's Support Services.

Zahoor, R., & Razi, N. (2020). Cyber-Crimes and Cyber Laws of Pakistan: An Overview. *Progressive Research Journal of Arts & Humanities (PRJAH), 2*(2), 133-143.