JURNAL UPI

Indonesian Journal of Multidisciplinary Research

IJOMR Indonesian Journal of Multidiciplinary Research

Journal homepage: http://ejournal.upi.edu/index.php/ IJOMR/

Ethical Issues of Cyberstalking and Personal Privacy in Pakistan: A Literature Survey

Atiya Sharf [1], Saeed Akhtar [1], Swera Sharf [2], Muhammad Asif [3,]*

[1]Riphah Institute of System Engineering, Islamabad, Pakistan.
[2]Department of Business Administration, University of Education, Lahore, Pakistan.
[3]Department of Environmental Science COMSATS University Islamabad, Abbottabad Campus, Abbottabad Pakistan
Correspondence: E-mail: 03047092647asif@gmail.com

ABSTRACTS

Electronic media is the fastest-growing technology of the modern era. Our society is relying on technological powers and lighting the fast speed of the internet to get maximum information about everything anywhere in the world. It plays a significant role in providing various facilities to the users but at the same time, personal privacy and cyberstalking issues must face. Cyberstalking is considering a major arising challenge to the modern world currently. Modification of technologies has a direct relationship with increase crimes of cyberstalking. This article represents a glimpse of unexpected activities like ethical dimensions of privacy, cyberstalking, and cyber harassment in Pakistan. Furthermore, the strategies associated with cyberstalking crimes, judicial involvement measures, and preventative proposals are also reported minimizing this emerging global crime.

ARTICLE INFO

Article History:
Submitted/Received 15 Jul 2020
First revised 19 Aug 2021
Accepted 20 Aug 2021
First available online 21 Aug 2021
Publication date 01 Sep 2021

Keyword:
Citizens,
Cyberstalking,
Ethical concerns,
Government responsibility,
Legal liability,
Moral obligation,
Personal privacy issues.

1. INTRODUCTION

There are questions:

(i) What is exactly cyberstalking and breach of personal privacy

(ii) How do the cases of violence in cyberspace apply to ethics?

For answering these research questions, we begin with the basic definition of stalking. Corresponding to Webster's New World Dictionary of the American Language, engaging in stalking is stealthily pursuing or approaching a game, an enemy, etc. as from the cover. In the sense of illegal activity involving human interaction, a stalking crime is commonly regarded as one in which an individual clandestinely monitors the actions of another person or entity. Most of our personal information like pictures, phone number, and even our current location is available on social media accounts. Most people do not understand that our social media accounts are very vulnerable to hacking and can result in identity theft. Many people do not protect their accounts appropriately they take it lightly. This can result in hacking of their account and theft and manipulation of the data.

Cyberstalking and harassment victims can be male or female; however, females are more prone to be affected by this horrible act. Women mostly get harassed on widely used social media platforms like Facebook and Instagram. Cyberstalking can be defined as a mode of action that extends to the online environment, those forms of stalking-related behaviors that have occurred in the past in the physical state. Cyberstalking is claimed that it's not a new kind of crime. Internet stalkers may act online anonymously or as a pseudonym. Furthermore, a cyber-stalker can stalk one or more people from their homes, so they don't have to venture out into the real world to stalk others. Therefore, internet technology offers stalkers the style of stalking that was not feasible in the pre-cyberspace era.

Recently, several people are concerned about the stalking activities that have happened in cyberspace, there are many explanations why these people seem justified in their concern. Because this crime, in general, is not fully clear in terms of its conceptual boundaries and their consequences, it is that much harder to understand exactly what it would mean to do a cyber-domain stalking crime. This research focuses on security issues of cyber-stalking and privacy, Firstly, how stalking victim's privacy is compromised by free access to the sensitive personal information available on the internet. Secondly, Cyber-stalking and personal information related to security cases in Pakistan are discussed. Lastly, examine the ethical and moral issues regarding the mention topics.

The objective of this study is to bring awareness to the public about cyberstalking. How people should use electronic communication mediums, e.g. social media, e-mails, and other communication channels. People use the Internet most frequently other than anything whether it is for work or fun. We cannot imagine the world without the internet, having lots of advantages it also has its dark side i.e. cyberstalking. The scope of this study was case studies related to privacy breaches, cyberstalking, cyber harassment, and cybercrime. Then, what kind of cyber laws are in practice in Pakistan and precautionary measures for people to cater to these cyber crimes?

2. LITERATURE REVIEW

The rising technologies of mobile and cloud computing, electronic commerce, and social applications are primarily changing the world's viewpoint. Around 43% of the world's populace presently has web get to, which is up from 6.5% in 2000 and the worldwide infiltration of mobile-cellular memberships has come to 97%. In the developed world, more than 80% of all family units have got to the web. By the conclusion of 2015, 3.2 billion

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN 2776-608X e- ISSN 2776-5970

individuals were utilizing the web all-inclusive of which 2 billion were from developing countries. This globalization of innovation encourages the ever-increasing chance of cybercrime. A survey of Fortune 1000 companies found a yearly development rate of 64% in cyber-attacks being carried out through the internet.

In Pakistan, the frequency of cybercrime has moreover been on the rise. Agreeing to official statistics, the instruction framework of Pakistan comprises nearly 0.26 million educate, and1.5million instructors who encourage around 41 million students. On the off chance that education is characterized as the ability to examined and type in one's title, it is around 69% in Pakistan. As the education rate increases, the number of individuals who can utilize the web will increment. Pakistan is positioned 27th within the world due to its web utilization as its citizens have an expansive social media impression. With increased utilization, come more noteworthy threats (Rauf, 2019). The level of awareness regarding online harassment laws in Pakistan is our 28% of women know that there is a law that exists against cyber-harassment and 72% don't know about any law of cyber harassment that exists in our country.

Although stalking has been a problem for many years, only in this decade has it received adequate attention from lawmakers, policy officials, and law enforcement agencies? According to a survey of online crimes that continue to target women in Pakistan 40% of women have been stalked and harassed via messaging apps. 72% of women do not know about cyber harassment laws in Pakistan. 70% are afraid of posting their pictures online. 45% of women think it's embarrassing to report online harassment. 47% don't report cases because they think it's not necessary.

For this research, the technique of information collection used were case studies, news articles, social media, online journals, other research papers, and reports published by the National Response Centre for Cyber Crime (NR3C). The objective of this research was to investigate in case any or being the victim of cybercrimes and whether they have reported any such incident. We have searched many databases including Google Scholar, Taylor & Francis, PubMed, and ACM digital library to get the top-cited papers related to our research topic. To have the understanding and insight of ethical issues related to cyberstalking and personal privacy. After a thorough search, we found these research papers and articles.

3. CASE STUDIES

The difficulty in understanding some essential features of cyberstalking crimes is that these crimes sometimes border on broader forms of cyberspace harassment crimes, and thus become confused with them.

a) In 2017 In Lahore, an FIA magistrate sentenced a man to six years punishment and a 0.7 million fine also imposed on him for harassing and blackmailing a woman online plus 1 million rupees payable for the victim by a prisoner under section 20(offenses against dignity), 21(offenses against modesty) and 24 (cyberstalking) of the Prevention of Electronic Crimes Act (PECA) 2016. That lady is the wife of a Pakistan air force officer and lived in Bahawalpur Pakistan. The culprit was indicted for cyber offenses which included digitally manipulating the victim's photographs, and in this way harassing and blackmailing her on social media. This judgment is taken very appreciable by the public. An excellent decision by the court set a new precedent for online harassment and criminal cases (Shariff, 2005).
b) Case from Karachi a 23- years old university student Maria had never been afraid of speaking ups about women issues in Pakistan. Her well- smooth, contentions to underpin women's rights were continuously praised by her companions, who would regularly tag her in social media posts related to women's liberation. And indeed, even though her

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN 2776-608X e- ISSN 2776-5970

contentions were never implied to be hostile, Maria rapidly got to be a victim of cyber harassment. "I never thought my suppositions would trigger Pakistani men to the extent that they would begin harassing me," Maria, who inquired to be distinguished as it were by her, to begin with, the title, told The Express Tribune. "Many men have begun sending me salacious and abusive messages on my Facebook and a few of them indeed replicated my pictures from my profile, undermining to specialist them fair since they did not agree with my views on women's rights". At first, Maria chosen to look for help and report her harassers to the cybercrime cell, but owing to family and peer weight, she changed her mind. "I truly needed to report the guilty parties for cyber badgering, but my mother and female companions demanded that I changed my security settings on Facebook and ceased straightforwardly sharing my views.

Indeed, even though self-censorship was discouraging, online trolls inevitably halted irritating me." Maria's experience with online harassers has been one of a kind, as thousands of Pakistani urban females are detailed to have experienced cyber harassment in one shape or the other on a day-to-day basis (Hafeez, 2014).

c. Man gets a 6-year jail term, Rs1.7 m fine for harassing women online

To guide people about harassment, a young promotor Usman Awan from Pakistan has stepped in to work against cyber harassment in Pakistan. He aims to work for the cultural, moral, and religious values of Pakistan and founded an anti-harassment campaign called "Stop Harassment Now."

4. CYBER CRIME LAWS IN PAKISTAN

Currently, there is no law to deal with cybercrime in Pakistan. This matter cannot be addressed simply by altering existing legislation and laws. It requires an advance, innovative, and wide-ranging legal structure that centers on the online conduct and behavior of individuals, administrations, and different organizations in the virtual world. The government has taken action to mitigate cybercrime issues. National Response Centre for Cyber Crime (NR3C) is the most recent mandate of the Federal Investigation Agency, basically to manage electronic and cybercrimes in Pakistan. FIA is the only agency in Pakistan that deals with this kind of crime and helps other law enforcement organizations in their cases. Prevention of Electronic Crimes Bill 2014 embraces fundamental, important, and technical requirements concerning electronic crimes are currently before the Cabinet. The introduction of this bill will avert cybercrimes and will add to national security while giving and empowering a healthy and safe environment in IT and e-Commerce. This bill will also consider the situation of citizens which has up to this point not been totally powerful, presenting them to unmitigated dangers presented by cybercriminals.

5. BUILDING AWARENESS IN PUBLIC

To make sure that your social media accounts are safe from people, make sure you follow these steps. Always enable verification steps to secure your information present in different databases, emails, and social media account(s). Use the phone number which is under your personal use for secondary verification. Use a difficult password that cannot be guessed easily and doesn't share your password with anyone. Always log in from trusted devices and never log in to your accounts from public computers. Several points must be considered:

(i) Strangers Can Be Dangerous. There have been various cases where people's accounts were hacked when they accessed a link sent by any stranger. If in case you receive a message from anyone who asks you to open a certain link and log in, never open it. These

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN 2776-608X e- ISSN 2776-5970

are fake pages created to hack your accounts as you enter your information or open it. Some links ask you to run a script on your laptop which can record the clicks on your keyboard and send information to the hacker from your laptop.

(ii) Never Share Personal Pictures and Videos. Although taking a photo of you in a public setting is not a violation of privacy, if the person takes your photo in your home and then uses it on social media without your information, you have legal recourse. Legal action can be taken against this. In some cases, personal data is used to blackmail the girl and posted online. To keep yourself safe from any such events, please do not share any personal pictures or videos with anyone. The objective of this clause is not to make you doubtful about your close ones. It is important to keep yourself safe from any regrettable event; you should keep certain material or information private. Apart from sharing, you should also avoid keeping your data on your mobile phone as well. In case of theft or loss, you will be a direct target to be blackmailed very easily.

(iii) Keep Yourself Unreachable for Offenders. Various applications and phone manufacturing services offer their user the facility to block unknown and annoying numbers. By blocking, you will not be annoyed by any offensive call or message. For the first time when a stranger sends you an aggressive message, you can either ignore it or add the number to the block list. However, keeping quiet in this matter is not a wise choice. Facebook also provides an option where you can remove the message and add a friend option from your profile if you don't want strangers to add you on social media.

(iv) Collect Proof to Lodge (Register) a Complaint. If you are a victim of online cyber harassment, make sure you have evidence to register a complaint against the offender. Take screenshots of the messages you have received and collect records, keep them in a safe place as evidence. Show the evidence and collected data to someone trustworthy and then report it to relevant organizations like the "National Response Centre for Cyber Crime" which is working against cyber harassment in Pakistan.

(v) Learn the cybersecurity laws. There are various cybersecurity laws to protect the victim from the offender. Problem is that most of us are not aware of these laws. Every person, whether who is a victim or not, should read all cyber harassment laws which tell everything about the punishment/ penalty of cyber harassment in detail.

(vi) Information Gathering. For this research, the technique of information collection used were case studies, news articles, social media, online journals, other research papers, and reports published by the National Response Centre for Cyber Crime (NR3C). The objective of this research was to investigate in case any or being the victim of cybercrimes and whether they have reported any such incident.

6. ETHICS IN CYBERSPACE

Considering ethical values and morals while using electronic media is the need of this age. We witness many cases that how people exploit internet technology and harm others. Hackers hack individual's social accounts, emails, phones, and laptops to get their personal information. Ask for ransom, selling personal data to companies, and getting money. Many hackers do cyberstalk, but it is more dangerous no one knows for what purpose they are stalking the public. Whether for money or some personal grudge, whatever the reason is people get hurt physically, mentally, emotionally, and financially. Pakistan's government should enforce cyber laws for public safety like awareness campaigns. Citizens themselves should start awareness campaigns to build awareness in people how to use the internet and

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN 2776-608X e- ISSN 2776-5970

electronic communication mediums. People must think about other's safety and welfare, respecting other's privacy.

6. CONCLUSION

This paper discusses the ethical and moral gaps in concerns in cyberspace, focusing on different cyberstalking and privacy breach-related incidents and cases. Sought to highlight the need for law for the electronic crime. Building awareness in people and attracting the attention of the Government to take practical actions. Different steps have been mentioned to help people protect themselves and their information from cyberstalking and privacy problems. Such crime happens when people get gadgets but don't know how to use electronic gadgets and electronic communication mediums. The government must start a campaign to educate citizens. Creating awareness of what cybercrime and cyberstalking are and what are the consequences of crimes would pay off in the long-term. Users should also be taught how to share information and not expose them to the entire world. Any individual commits the offense of cyberstalking who, with the expectation to obtain personal information, threaten or harass any person, uses any electronic medium whether it is a website, e-mail, social accounts or any other comparable implies of communication should get severe punishment.

7. AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the paper was free of plagiarism.

8. REFERENCES

Hafeez, E. (2014). Cyber Harassment and Its Implications on. *Horizons*, *8*(2), 29-48.

Rauf, S. (2019). Role of Youth in the Promotion of Good Governance in Pakistan. *Journal of Political Studies*, Special Conference Issue, 43-54.

Shariff, S. (2005). Cyber-dilemmas in the new millennium: School obligations to provide student safety in a virtual school environment. *McGill Journal of Education/Revue des sciences de l'éducation de McGill*, *40*(3), 457-477.

DOI: http://dx.doi.org/10.17509/xxxx.xxx
p- ISSN 2776-608X e- ISSN 2776-5970