Journal of Management Info

Journal Homepage: http://readersinsight.net/JMI

Research Article

Social networking privacy issues, legal concerns, and weak legislation a way to cybercrimes: A case of Pakistan

Mehwish Iftikhar[1]*, Zarina Waheed[2], Usman Abdullah[3], Sheraz Khan[4]

[1]NUST Business School, National University of Sciences and Technology, Islamabad, Pakistan
[2]Education Department, Sardar Bahadur Khan Women's University, Quetta, Pakistan
[3]Department of Management Sciences, COMSATS University Islamabad, Islamabad, Pakistan
[4]Judicial Magistrate, Peshawar High Courts, Peshawar, Pakistan

*Corresponding Author email: mehwish.iftikhar@nbs.nust.edu.pk

Submitted: 14 October 2022 *Revised: 22 December 2022* *Accepted: 30 December 2022*

ABSTRACT

Extension of information & communication technologies elevated the necessity for more confidentiality of data and its protection against cybercrime. More so, advancement in ICT is beneficial whereas on the contrary, due to its excessive utilization the privacy and legal/security crisis are at stake. This qualitative study, using grounded theory analysis approach, explores how social networking privacy issues, legal concerns and weak legislation lead to cybercrimes in Pakistan. For this purpose, social networking sites, documents, relevant literature and interviews were used as data collection tools. The findings indicate that the social networking big data contains various legal issues such as privacy and security. Moreover, due to weak legislative laws, such issues are promoting cybercrimes such as cyberbullying, cyber stalking, cyber defamation etc. in Pakistan, which may have adverse and devastating effects.

Keywords: *Social Networking; Legal Issues; Legislative Laws; Cybercrimes*

1. INTRODUCTION

Today world is in the era of "big data". The digital networks have transformed the ability to produce, share, and access data by connecting the increasing number of people and devices. The available transactions, email, videos, images, logs, search queries and the health records, social networking connections are producing big data, which is gathered from increasingly persistent sensors installed in organization, in homes, and in the mobile phone (Tene, 2011). Social networking sites are the source of wide amount of data and its sharing, became a prevalent medium of data dispersion (Almadhoor, 2021). Social networking has its crux from different platforms of Facebook, Twitter, and LinkedIn & many others. Facebook leads the list among the biggest social networking sites by getting above than 175 million active users in its first five years. According to Akhlaq (2021), in Pakistan there are about 35 million active Pakistani users of Facebook, which is quite a high ratio. And the strength of overall internet users in Pakistan has increased by 11 million in one year from 2020 to 2021. People can interact in these networks, manage their profiles, and can

https://doi.org/10.31580/jmi.v9i4.2844

have their own family circles, and share their opinions, perceptions, info, knowledge, and views with each other (Peng et al., 2017). However, the increasing use of social media networking has posed a biggest data challenge, and this has led to generation of quite a few concerns, including privacy Cerruto et al. (2022) and security Soomro and Hussain (2019), issues. The collection of bulky sets of private data and the usage of state-of-the-art analytics incriminates rising privacy concerns (Solove, 2006). Multiple type of related info on personal home pages/blogs may contain private data such as birth dates, home addresses, and personal mobile numbers etc. This info can be hacked by hackers to be used for their own benefits (being misused) and steal money, using social engineering techniques (Ghari & Shaabi, 2012; Khan, 2015).

In Pakistan, for educational, commercial, and non-commercial purposes many users are using social networks as a communication tool. These social networks have been reported to have some constraints regarding data security, user privacy, data integrity, fake accounts, fabricated videos, unauthenticated information, un-necessary ads, data accessibility and interface interoperability issues (Hussain et al., 2016). In addition to this, the excessive use of social networking leads youngsters to be indulged in cybercrimes (Meter & Bouman, 2015; Gupta et al., 2016) or to be the victim of it. And the research by Ganesh et al. (2020), proved that, unfortunately internet users are having very low level of knowledge related to cybercrimes and its occurrence. Among the fastest growing areas of criminality, cybercrime is taking the lead (Goni et al., 2022). Cyber space has been subjugated by many fields of study; though, criminology was too late to investigate cybercrime. There are four major categories for cybercrimes which are cybercrime against individuals, cybercrime against property, cybercrime against organization and cybercrime against society (Jaishankar, 2018). As per Goodman and Brenner (2002), cybercrimes against individuals are hacking, email spoofing, spamming, cyber defamation and harassment, cyber stalking and cyber bullying. Due to these new forms there is a challenge to lawmakers and law implementation agencies (Halder, 2011) to make such laws which can tackle with these issues.

Cyber-legislation is the only solution to monitor; control and prevent cybercrimes. In the entire world, countries are at stake to threats of cybercrimes due to various reasons, which are ranging from the unavailability of legislation to financial restrictions and the absence of cooperation with international law and administering organizations (Kundi et al., 2014). Furthermore, globally, the current legislation is not capable of dealing with cybercrime, resultantly, the criminals are taking it as an incentive and they continue to commit such crimes. Cybercrime is a heated debate round the world, same like other nations in the world, Pakistan is also vulnerable to its implications Mateen and Abbas (2016), and is struggling to omit it using critical legal policies.

Thus, managing privacy is effectively both a psychological and a sociological problem especially on social networking sites, which must be addressed jointly from both perspectives to realize the promise of big data, so the current study is doing. In addition, this study is also exploring the role that cyber-legislation can play in controlling cybercrimes in Pakistan.

2. MATERIALS AND METHOD

This study opted qualitative method. The trustworthiness in qualitative studies was assured via triangulation (Miles & Hubberman, 1994). Through purposive sampling, 4 judges and senior lawyers and 4 users of Facebook and twitter social networking who have been the victims of any kind of cybercrime through social networking were selected. The data was collected through documents and semi-structured interviews. For document analysis press release, newspapers, social media sites were used and analysed. Facebook and Twitter have high usage in Pakistan and among youth therefore only those were selected as big data sites for data collection.

2.1. DATA ANALYSIS

The data was analysed by using grounded theory analysis technique (Corbin & Strauss, 2008). The documents and interview transcriptions were uploaded in ATLAS.ti. 7 for analysis. Fig.1 below presents the summary of research method and four steps of grounded theory analysis used:

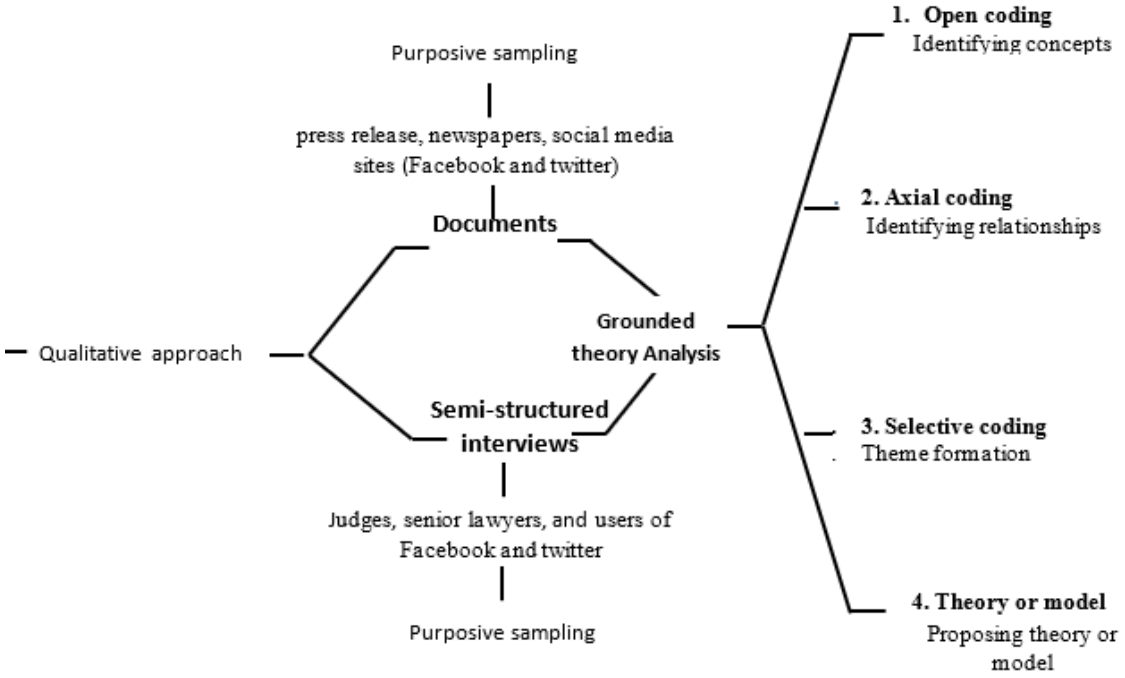

Fig. 1. Summary of the research method.

3. FINDINGS AND DISCUSSION

The data analysis revealed that comments posting, sharing of photos, aggressive memes and videos were considered as the source of detection of criminal activity.

3.1. USE OF SOCIAL NETWORKING SITES IN PAKISTAN

A review of documents analysis indicated an increasing ratio of social media websites users in Pakistan. Social media sites provide the platform to the common public to speak up and share whatever they want. Same is with Pakistan, as participant claimed:

> Pakistani nation is suffering from bad governance and corrupt leadership. In such kind of situation, common people of the country got overlooked, at this time digital and social media provides such kind of platforms to common people where they may come and speak for their rights. Social media platform provides the true freedom of speech to common people as well as the power to their opinions.

A report shows the statistics that by January 2019, out of 198.9 (total population of Pakistan) there are only 44.6 million internet users which shows that about only 22% of total population of Pakistan have internet access and only 18% (35 million) are an active social media user on different websites of social networking (Farooq, 2019). Stats also shows that 32 million users out of 35 million access the internet by their mobile devices.

The six most commonly used social media websites on the internet by the people of Pakistan are: Facebook, Twitter; YouTube; Twitter; Instagram; Pinterest and Google+. Statistically the most frequently used social networking big data sites are Facebook, YouTube and twitter (92.06%, 4.68% and 1.50%) in Pakistan (Alphapro.pk). A famous networking site Facebook has the highest percentage of usage as there are total 35 million active Pakistani users (monthly) and the ration has increased by 17 % annually in 2017.

3.2. Weaknesses of PECA Act

In 2016, Pakistan's Government passed the "Prevention of Electronic Crimes Act, 2016" law (Prevention of Electronic Crimes Bill, 2016). The Act described that the legislation has the purpose to prevent unauthorized acts related to Information Systems and to trace out the related crimes and to provide a proper mechanism to investigate and prosecute the offense, as well as for trial and international cooperation. However, the law still has shortcomings as according to (Mohammed, 2015) legislation is quite weak and does not deal comprehensively with the growing threats of cybercrime and fails to tackle with the online violence (Oxford Analytica, 2022). The data analysis revealed that the activists of human rights as well as free speech are concerned and worried about cyber laws (Bolo Bhi, 2016) as they exposed that "lots of provisions of the PECA are outlined and introduced by using vague terminologies, which may violate or restrict the free speech rights and lead towards unfair prosecutions". (Zahra-Malik, 2016). The initiator of the Digital Rights Foundation, Nighat Daad was quoted as stating that "the language used in the bill is overly broad which ensures that ignorant/innocent people of Pakistan cannot understand the ramifications of the bill and its entailment and may consider themselves as a subject to very strict penalties." (Id.) Practitioners have criticized PECA in terms of its implications as it provides immense power to authorities which are violate of due process of law which may lead towards abuse of the law (Sridharan, 2016).

Opposing political parties also uttered their concern about the misuse of the Act by the representatives of the government and are worried that there is a possibility of stifling online political debate (Magalla, 2018)

The Judges and senior lawyers were having the common views on PECA and its implementation in Pakistan to eliminate cybercrimes as a Judge explained:

> Prevention of Electronic Crime bill is quite harsh regarding to punishments, punishments do not fit specific cybercrimes. The Act restricts the free speech and the language is so ambiguous and is difficult to understand for common people.

Other senior lawyer, shared his views upon cybercrime act and said, "this law cannot differentiate between cybercrime, cyber terrorism and cyber warfare. The wording of the bill is not that clear and is open to interpretation". "The law is given power to authorities to block and destroy the online content without getting permission from the court, this can be problematic thing in this Act", another Judge added. The second senior lawyer argued, "in spite of having so many amendments in PECB- Prevention of Electronic Crimes Bill, even more then 50, by the Senate which the National Assembly been adopted as well but always remain a controversial legislation".

Thus, the findings show that most of the terminologies used in PECA bill are vague and imprecise and the proper implementation of the Act is missing as well.

3.3. Analysis of National Response Centre for Cybercrimes

In order to combat against cybercrimes, National Response Centre for Cybercrimes (NRC3-FIA) was emerged with professional competence. NRC3 - FIA is the only law enforcement agency devoted to fight against cyber/electronic crimes in Pakistan, initiated in 2007. The agency tries to limit the occurrence of technological abuse in digital networking society and mainly deals with the technology-based crimes in Pakistan.

The data analysis of webpages of cybercrime wing-FIA shows the increasing percentage of cybercrime acts and the dissatisfied performance of NR3C-FIA. People commented about their complaints and the responses of cybercrime wing personnel. One person commented that:

> I have reported a cyber-fraud and sad part is that even police personnel and those who were affiliated with Nr3c were saying that they will not give it much priority and the whole process will take a lot of time".

The other victim said:

> I became the victim of cybercrime few months ago, someone hacked my personal account and was posting wrong things on my behalf...I complaint to cybercrime wing-FIA but they didn't reply. I was calling again and again but they even did not receive my call, the whole act made me so depressed.

There are various examples, people endeavoured to get help from this wing regarding to cybercrimes but all in vain. Another person commented about the performance of cybercrime wing Lahore as, "...I have been complaining to cybercrime wing for two years as I had been consistently cyberbullied by someone, but I neither receive any kind of help nor justice. People sitting in that wing are corrupt and unjust". The V3 shared her experiences of cyberbullying as:

> … I have passed through a very bad experience of continues bullying on Facebook for two months. An anonymous person was using an abusive language and giving me the threats of killing for unknown reasons. I couldn't even share with my family or friends which lead me to severe mental health issues. Right after two months he vanished.

The excerpt above shows that many cases of cybercrimes are even not reported in NRC3 – FIA. The V2 passed through the experience of her twitter account hacking where she had lots of personal pictures and videos which were misused by a hacker later on. The V4, on the other hand said that she had reported a case against a fake Facebook account using her name and pictures in FIA with support of her family members. She added:

> …after few months I went back to FIA Quetta office to inquire about my case, surprisingly, they said the officer has been changed and if you want this officer to solve your case you need to report again… then I did not go back…even after few months a WhatsApp group with "sexy girls" name was created with pornographic pictures, I was added into it, I simply reported this to my brother and husband only (laughing).

The analysis of comments on FIA websites and interviews of social networking site users revealed that people of different cities of Pakistan are the victims of different kinds of cybercrimes such as cyberbullying, cyberstalking, cyber hacking, cyber frauds etc. They are not satisfied with the performance of cybercrime wing-NR3C which is to serve the nation on the basis of professional training and expertise.

3.4. Weak cyber legislation as a moderator

The analysis also depicted that there are weak legislative laws regarding to cybercrime acts in Pakistan due to which the ratio of cybercrimes is increasing day by day. The cyber-crime laws in Pakistan are still in the beginning phase . In this regard a senior lawyer claimed, "adequate and equipped Legal Frameworks can work in this regard". A judge added:

> … PECA, if implemented successfully after updating and improving the law and creating a separate agency for countering and controlling the cybercrimes, as promised in law; definitely will reduce cybercrimes.

Thus in the absence of cyber-law, online community is vulnerable to cybercrime, which is easily falling a prey to their wicked tactics, being deprived of privacy, data and money and also in few cases, a huge blow to their social and family life (Magalla, 2018). Hence it is concluded that weak legislative laws act as a moderator between social networking legal issues and cybercrime acts.

4. CONCLUSION AND PROPOSED MODEL

Findings emerged from the current study concluded that, with the ongoing increasing ratio of active online users in Pakistan the issues of privacy and security are increasing with the same pace which was quite significant to address. After reviewing the legislative laws it is pointed out that the current cybercrime law of Pakistan is not comprehensive and

mature in terms of dealing with the rapid increasing threats of the crimes done through digital means specially on social networking sites (Akhlaq, 2021), nor the cybercrime agencies are able to counter with the cybercrime acts properly which happened online and completely satisfy the victims with their efficient performance. Pakistan is lacking with the adequate and equipped Legal Framework which could efficiently address the online/virtual threats of current digital world. Cybercrime laws in Pakistan are unsatisfactory and fragmented. Lastly, because of weak legislation and poor performance of cybercrime agencies, the use of social networking sites lead users towards the commencement of cybercrime acts hence, the weak legislative laws act as a moderator between social networking legal issues and cybercrime acts. Based on data analysis, the following model shown in Fig. 2 is emerged which can be a significant contribution of this study:

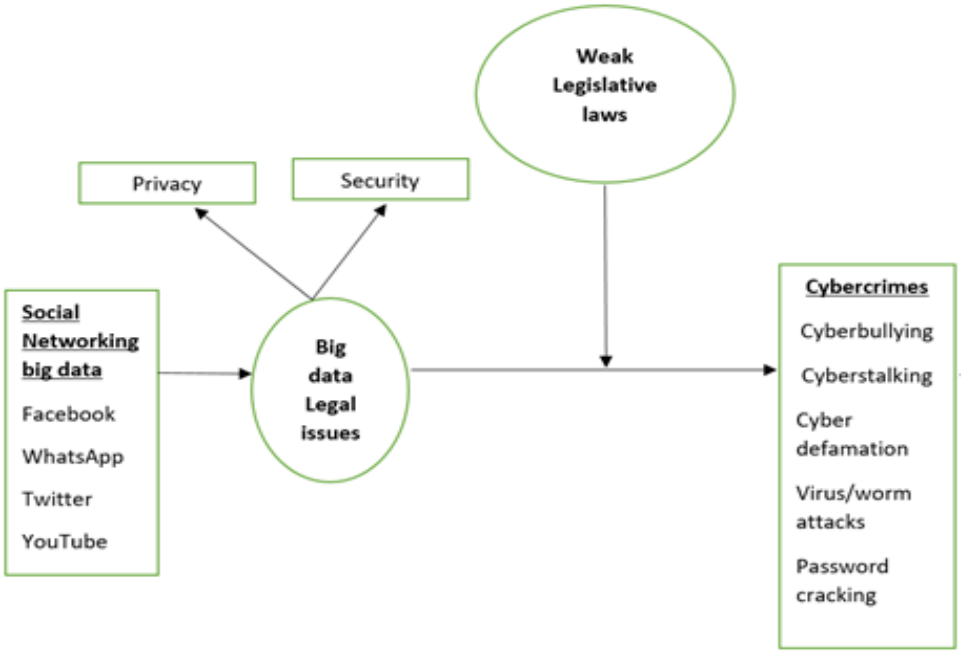

Fig. 2. The proposed model emerged from data analysis.

5. THEORETICAL AND PRACTICAL CONTRIBUTION

This study provides a meaningful extension to the work on cybercrimes in the management literature with the amalgamation of legal perspective. So far, relevant literature has a strong focus on analysing the concept of cybercrime in terms of its prevalence and statistics (Khiralla, 2020; Alelyani & Kumar 2018) and were mostly conducted in western countries (Hernandez-Castro & Boiten, 2014; Monteith et al., 2021) and have paid less attention towards knowing the reasons/causes. This research highlighted the legal issues as the antecedents and weak legislative laws as the moderator, by thoroughly studying PECA and its shortcomings and poor performance levels of cybercrime agencies specifically in Pakistan. These may work as the major contributors in the enhancement of cybercrimes on various social networking sites. The present study thus constitutes an important step forward in the development of framework showing the relationships between social networking legal issues and rising percentage of cybercrimes with the moderating effects of weak legislative laws.

This study can be obliging for the legal practitioners to know about the users' privacy and legal concerns related social networking sites, awareness about the inadequacies and deficiencies of legal laws and performance of legal agencies, so that they can regulate the criminal behaviours by making amendments in cyber laws and keeping the check on cyber agencies which can ultimately be helpful in cyber policy making.

6. FUTURE RESEARCH AVENUES

Cybercrime perspective is not limited only to these social networking websites, it would also be valuable if more networking sites and apps are added and vital to explore social issues as well, other than legal. The authors suggest future researchers to conduct more quantitative studies on the current topic to add up the knowledge and test the conceptually developed framework of the current study in different cultures and countries for further use. Multi-country analysis may also give a greater depth to the topic.

Author Contributions:

This section provides the detail regarding contribution by each individual in order to complete the research and making the final draft. Conceptualization, Mehwish Iftikhar and Sheraz Khan; Methodology, Mehwish Iftikhar and Zarina Waheed; Formal Analysis Sheraz Khan, Usman Abdullah, Mehwish Iftikhar; Zarina Waheed, Usman Abdullah; Writing-orignal draft preparation, Mehwish Iftikhar, Zarina Waheed and Usman Abdullah; Writing review and editing Sheraz khan and Usman Abdullah. All the authors read and agreed to the published version of the manuscript.

Funding:

This research received no external funding.

Institutional Review Board Statement:

N/A

Informed Consent Statement:

N/A

Data Availability Statement:

N/A

Acknowledgments:

N/A

Conflicts of Interest:

No conflict of interest

Reference:

Akhlaq, M. A. R. I. A. (2021). Cybercrime in Pakistan: A Study of the Law Dealing with Cybercrimes in Pakistan. *PCL Student Journal of Law*, *V*(1), 31-66.

Alelyani, S., & Kumar, H. GR, (2018). Overview of cyberattack on saudi organizations. *Journal of Information Security and Cybercrimes Research*, *1*(1), 32-39. https://doi.org/10.26735/16587790.2018.004

Almadhoor, L. (2021). Social media and cybercrimes. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 2972-2981. https://doi.org/10.17762/turcomat.v12i10.4947

Bolo Bhi. (2016). Major contentions: PECA' last accessed 16 March 2021

Cerruto, F., Cirillo, S., Desiato, D., Gambardella, S. M., & Polese, G. (2022). Social network data analysis to highlight privacy threats in sharing data. *Journal of Big Data*, *9*(1), 19. https://doi.org/10.1186/s40537-022-00566-7

Corbin J, Strauss A (2008). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. 3rd ed. SAGE

Farooq M. (2019), Active social media users in Pakistan grow by 5.7%: Report. *Pakistan Today*. https://www.digitalrightsmonitor.pk/active-social-media-users-in-pakistan-grow-by-5-7-report/. Published 2019.

Ganesh, S., Ganapathy, D., & Sasanka, K. (2020). Awareness of Cyber Crime on Social Media. *Journal of Contemporary Issues in Business and Government*, *26*(2), 1758-1765

Ghari W. & Shaabi, M. (2012). Cyber Threats In Social Networking Websites. *International Journal of Distributed and Parallel Systems (IJDPS), 3*(1), 119-126. DOI:10.5121/ijdps.2012.3109

Goni, O., Ali, M. H., Alam, M. M., & Shameem, M. A. (2022). The Basic Concept of Cyber Crime. *Journal of Technology Innovations and Energy*, *1*(2), 16-24

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International journal of law and information technology, 10*(2), 139-223. https://doi.org/10.1093/ijlit/10.2.139

Gupta S, Singh A, Kumari S, & Kunwar N. (2017). Impact of cyber crime on adolescents through social networking sites. *International Journal of Law 3*(6), 104-106.

Halder, D. (2011). Information Technology Act and cyber terrorism: A critical review. *Available at SSRN https://ssrn.com/abstract=1964261* OR http://dx.doi.org/10.2139/ssrn.1964261

Hernandez-Castro, J., & Boiten, E. (2014). Cybercrime prevalence and impact in the UK. *Computer Fraud & Security*, *2014*(2), 5-8. https://doi.org/10.1016/S1361-3723(14)70461-0

Hussain, Z., Bhutto, Z. A., Rai, G., Hussain, M., & Zaheer, K. (2016). Statistical analysis of network based issues and their impact on social computing practices in Pakistan. *Journal of Computer and Communications*, *4*(13), 23. DOI: https://doi.org/10.4236/jcc.2016.413003

Jaishankar, K. (2018). Cyber criminology as an academic discipline: history, contribution and impact. *International Journal of Cyber Criminology, 12*(1), 1-8. DOI: https://doi.org/10.5281/zenodo.1467308

Khan, T. (2015). Cybercrimes: Pakistan lacks facilities to trace hackers. T*he Express Tribune*.

Khiralla, F. A. M. (2020). Statistics of cybercrime from 2016 to the first half of 2020. *International Journal of Computer Science and Network., 9*(5), 252-261.

Kundi, G. M., Nawaz, A., Akhtar, R., & MPhil Student, I. E. R. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications*, *4*(4), 61-71. doi:http://www.iiste.org/Journals/index.php/JIEA/article/viewFile/12430/12764

Magalla, A. (2018). Prevention and detection of cyber crimes in tanzania as described by cyber crime act, no. 13 of 2015. http://dx.doi.org/10.2139/ssrn.3136637

Mateen, A., & Abbas, Q. (2016). Tsunami of Cyber Crime: Analysis of Cyber Crime New Trends, Causes and Remedies in Future Prospectus. *International Journal of Computer Applications*, *152*(8).

Meter, D. J., & Bauman, S. (2015). When sharing is a bad idea: The effects of online social network engagement and sharing passwords with friends on cyberbullying involvement. *Cyberpsychology, Behavior, and Social Networking*, *18*(8), 437-442. https://doi.org/10.1089/cyber.2015.0081

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

Mohammed, F. (2016). PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill. *UCLA J Islam Near EL*, *15*, 71.

Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current psychiatry reports*, *23*, 1-9. https://doi.org/10.1007/s11920-021-01228-w

Oxford Analytica. (2022). Pakistan, Bangladesh fail to tackle online violence. *Emerald Expert Briefings*, (oxan-db). https://doi.org/10.1108/OXAN-DB266467

Peng, S., Wang, G., & Xie, D. (2017). Social influence analysis in social networking big data: Opportunities and challenges. *IEEE network, 31*(1), 11-17. https://doi.org/10.1109/MNET.2016.1500104NM

Prevention of Electronic Crimes Bill 2016.; (2016). http://www.na.gov.pk/uploads/documents/1470910659_707.pdf

Solove, D. J. (2006). Taxonomy of Privacy. *University of Pennsylvania Law Review*. *154*(3), *477*. GWU Law School Public Law Research Paper No. 129, Available at SSRN: https://ssrn.com/abstract=667622

Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. *Applied Computer Systems*, *24*(1), 9-17. DOI:10.2478/acss-2019-0002

Sridharan, V. (2016). Pakistan passes 'draconian' cybercrime law threatening civil liberties. *International Business Times*. https://www.ibtimes.co.uk/pakistan-passes-draconian-cybercrime-law-threatening-civil-liberties-1575530. Accessed August 23, 2020.

Tene, O. (2011). Privacy: The new generations. *International data privacy law, 1*(1), 15-27. https://doi.org/10.1093/idpl/ipq003

Zahra-Malik, M (2016). Pakistan passes controversial cyber-crime law. *Reuters*. https://www.reuters.com/article/us-pakistan-internet/pakistan-passes-controversial-cyber-crime-law-idUSKCN10N0ST.