TACKLING CYBERAGRESSION FROM A GENDER BASED VIOLENCE PERSPECTIVE IN LESOTHO: A PLEA FOR LEGISLATIVE INTERVENTION

Nthabeleng Charlotte Maebo

Supervised by: Advocate Mothepa Ndumo

A Dissertation Submitted to the Faculty of Law in Partial Fulfilment of the Requirements for the Award of the Degree of Bachelor of Laws (LLB).

National University of Lesotho

2020

DECLARATION

I declare that *Tackling cyberagression from a gender based violence perspective in Lesotho: a plea for legislative intervention* is my work, that it has not been submitted before for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged as complete references.

Nthabeleng Maebo 2020

ACKNOWLEDGEMENTS

This work is dedicated to the memory of my grandmother, ‘Mathabang Tseko a working class hero.

I would also like to thank my Mother and Father who have always been there for me.

Above all, I thank God, the only Man that has been with me every step of the way, and the one that is always by my side.

I would also like to thank my supervisor, Advocate Mothepa Ndumo, for the valuable supervision throughout.

Last but not least, I am grateful for all my friends who have supported me and given me hope even when I had lost it.

TABLE OF CONTENTS

TOPIC **1**

DECLARATION **2**

ACKNOWLEDGEMENTS **3**

CHAPTER 1: INTRODUCTION TO CYBER AGGRESSION AND THE LAW……6

1.1. Introduction……..6

1.2. Background……..9

1.3. Statement of the problem……..10

1.4. Aims and objectives ……11

1.5. Methodology……12

1.6. Hypothesis……13

1.7. Synopsis of subsequent chapters……14

CHAPTER 2: CYBER HARASSMENT IN THE WORKPLACE AND IN HIGHER EDUCATION INSTITUTIONS……16

2.1. Introduction……16

2.2. Literature review……16

2.3. Legal framework of other jurisdictions……21

2.3.1. Domestic framework……21

2.3.2. African Union……24

2.3.3. SADC……25

2.3.4. Global framework……..25

2.4. Conclusion……26

CHAPTER 3: COMPARATIVE STUDY…….27

3.1. Introduction…….27

3.2. Legal framework of workplace cyber harassment in Lesotho compared to South Africa……..27

3.3. Legal framework of workplace cyber harassment in the United States of America…….29

3.4. Case law on workplace violence and higher learning institutions……..31

3.5. Critical examination of the Computer Crimes and Cyber Security Bill of 2020……..33

3.6. Conclusion……35

CHAPTER 4: CONCLUSION AND RECOMMENDATIONS……....36

4.1. Introduction……....36

4.2. Findings……..36

4.3. Conclusion……..37

4.4. Recommendations……..38

BIBLIOGRAPHY……....42

CHAPTER 1: INTRODUCTION TO CYBER AGGRESSION AND THE LAW

1.1. INTRODUCTION

Workplaces and higher education institutions in Lesotho have seen a rise in aggressive forms of interactions online; social media has become the main platform that facilitates the invasion of people's privacy and the marginalization of their human rights. The lack of a legal framework that addresses these cyber-aggressions therefore requires urgent intervention as our society becomes increasingly sophisticated.

There are many forms of cyber-aggressions, including cyberterrorism, but this dissertation is mainly focused on online aggressions with overtly sexual elements including cyber harassment, cyberstalking and revenge porn and the problems that these occurrences create for people in workplaces and higher education institutions in Lesotho. It should be emphasized that cyber harassment is also used as a catch-all phrase for online aggressions with a sexual undercurrent. Having realized that Lesotho has limited laws on cyber harassment, this dissertation proposes that the legislature should interfere and enact laws that will protect cyber harassment victims.

The dissertation provides background information about cyber harassment, defines the problem and where it is focused, examines the legal issues that surround the forms of cyber harassment, and discusses possible preventative programs from a legal perspective.

The researcher intends to evaluate the legal frameworks of different jurisdictions in order to draw comparisons between Lesotho and best practices globally. The first process, which will come under the microscope of this dissertation, shall involve the

unresolved cases that are well known but remain unreported in Lesotho. The second process that shall be examined is Lesotho's legal position and legal framework governing cyber harassment. The laws that are relevant to cyber harassment in Lesotho are, according to the researcher, scattered and do not address these new forms of harassment directly. These scattered pieces include Codes of Good Practice [1] and the Labour Code Order. [2] In highlighting their shortcomings, section 59 of the Codes of Good Practice describes the forms of sexual harassment in the workplace but does not include that sexual harassment can take place through cyber-space in the form of cyberaggression. On the other hand, section 200 of the Labour Code Order gives a broad meaning of sexual harassment, it does not specify that sexual harassment can be by means of cyberstalking with a sexual undercurrent. These abovementioned shortcomings are in relation to the new forms of online aggressions that people are increasingly becoming vulnerable to.

The Computer Crimes and Cyber Security Bill of 2020[3] is however intended to address a number of online security issues facing Basotho and Lesotho and, as shall be illustrated in Chapter three, this Bill is the first attempt in our jurisdiction to address cyber-aggressions of various forms. On many occasions, Basotho women and men, not forgetting children and young adults, are faced with the commission of cyber harassment. People of both genders, regardless of age, are affected by cyber-harassment, particularly in workplaces and higher education institutions where there are evidently many occurrences.

1.1.1. Definition of cyber harassment

[1] Lesotho Government Notice No.4 of 2003, Labour Code (Codes of Good Practice)
[2] Lesotho Labour Code Order, No.24 of 1992
[3] Computer Crimes and Cyber Security Bill 2020

Cyber harassment refers to online harassment. Cyber harassment is the use of email, instant messaging, and derogatory websites to bully or otherwise harass an individual or group through personal attacks.[4] Cyber harassment involves the use of ICT to intentionally humiliate, annoy, attack, threaten, alarm, offend and/or verbally abuse individuals.[5] In this dissertation, the researcher focuses on cyber harassment with sexual nuances. As stated previously, the term cyber harassment is also used as a catch-all phrase in this dissertation.

1.1.2. Definition of revenge porn

Revenge porn represents another form of cyber harassment, one with increasing visibility in the criminal and legal sector and it is also referred to as the publication of sexually explicit images or videos on an online forum without the consent of the subject.[6]

Revenge pornography is a subset of image-based abuse, including both the non-consensual sharing and creation of sexual images, for a variety of motives, ranging from sexual gratification to harassment, control, and extortion.[7]

1.1.3. Definition of cyberstalking

Cyberstalking definitions vary, although the practice is typically understood as the repeated pursuit of an individual using electronic or internet–capable devices.[8] Cyberstalking involves the use of information and communications technology (ICT) to perpetrate more than one incident intended to repeatedly harass, annoy, attack, threaten, and/or verbally abuse individuals.[9] In the context of this research,

[4] https://definitions.uslegal.com/c/cyber-harassment/
[5] https://www.unodc.org
[6] Citron DK, Franks MA. 2014. "Criminalizing revenge porn. Wake Forest Law Rev. 49,345-391.
[7] Prof Davidson. J, et al, 2019. Adult Online Hate, Harassment and Abuse "*A rapid evidence assessment*"
[8] Drebing H, Bailer J, et al.2014 "Cyberstalking in a sample of social network users: Prevalence, characteristics, and impact upon victims. Cyberpsychol Behav Soc Netw. 17,61-67
[9] https://www.unodc.org

the term cyberstalking is limited to instances where a victim is repeatedly pursued via sexually suggestive or aggressive means online. To some extent, cyberstalking is fundamentally an extension of traditional stalking in which the offender utilizes a high-tech modus operandi to committing the crime.[10]

1.2. BACKGROUND

The incorporation of cyber harassment laws is a complex one because the Basotho Nation is ignorant about cyber harassment, therefore the lawmakers of this country wouldn't know when to interfere and when not to. Notwithstanding that research has been undertaken on harassment in Lesotho, relatively little is said about cyber-harassment as Lesotho's laws are sometimes behind the times.[11] Sexual harassment may occur as a result of cyber harassment. Section 59 of our Codes of Good Practice [12] mentions the forms of sexual harassment, but they did not include that sexual harassment can occur through cyber harassment.

Tackling these forms cyberaggression would not be such a difficult task if Lesotho had laws that govern them. In some cases, a cyber harassment victim gets to know the perpetrator, therefore, they can decide to open a case against them and seek the intervention of the lawmakers of this country to incorporate cybercrime laws in to Lesotho's laws. Since the Internet was first established in the late 1960s it has become significantly easier to gain access to email, bulletin board systems, and internet gaming.[13] Like most traditional crimes, cyber harassment knows no

[10] https://www.cybercrimejournal.com/pittaroijccvol1is2.htm
[11] Lekena. M, "An exploration of learners' experiences of bullying as an act that promotes exclusion in a high school in Botha-Bothe district, Lesotho.(Master of Education, Faculty of Humanities: University of the Witwatersrand)
[12] Codes of good practice) Notice 2003
[13] Budde, R. 2014, taking the sting out of revenge porn: Using criminal statutes to safeguard sexual autonomy in the digital age. Georgetown Journal of Gender and the Law, Forthcoming.

boundaries, anyone can become a stalking victim, whether it is random or predicated on poor judgment when one releases personal information on the Internet.[14]

1.3. STATEMENT OF THE PROBLEM

The problem is that Lesotho's government has only drafted a Bill on Computer Crime and Cyber Security of 2020 which is not yet enforceable because it is not an Act. There is very little or no jurisprudence/ case law on cyber harassment in Lesotho. The major limitation to implementing solutions to this problem is that Lesotho has inadequate resources. Therefore, the solution to this problem will only succeed on the back of adequate financial support and infrastructure.

According to Petrocelli, cyberstalking crimes present a unique challenge to law enforcement, particularly to those departments that lack the expertise or resources to investigate and prosecute cyber stalkers.[15] Local law enforcement is at a particular disadvantage as a result of jurisdictional limitations, for example, a stalker may be in another city, state, or even country, thereby making it difficult if not entirely impossible to investigate and prosecute.[16]

The anonymity of the Internet also places the cyber stalker in a truly advantageous position over law enforcement investigators.[17] Another problem is that no multilateral and regional treaties exist that cover cyberstalking and other forms of cyber harassment.[18] Some countries do have national laws that directly cover one or more of these cybercrimes; for example, Pakistan's Prevention of Electronic Crimes

[14] Michael L. Pittaro, 2007." Cyber stalking: An Analysis of Online Harassment and Intimidation."

[15] Petrocelli, J. (2005). Cyber stalking. Law & Order, 53(12), 56-58

[16] Petrocelli, J. (2005). Cyber stalking. Law & Order, 53(12), 56-58

[17] Reno, J. (1999). 1999 report on cyber stalking: A new challenge for law enforcement and industry. Retrieved Feb. 18, 2006, from United States Department of Justice Web site: http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm

[18] https://www.unodc.org

Ordinance of 2007, and Nigeria's Cybercrime Act of 2015 criminalize cyberstalking and Singapore's Protection from Harassment Act of 2014 proscribes cyber harassment.[19] Nigeria, Pakistan and Singapore are just being cited as examples and are not part of the comparative analysis of this dissertation in Chapter 3.

This dissertation also focuses on people in higher education institutions and in the workplace. Anecdotal evidence seems to suggest that cyberstalking and cyber harassment occur mostly in the workplace, while revenge porn occurs more often in higher education institutions.

1.4. AIMS AND OBJECTIVES

The main objective of this study is to emphasize and show reasons why Lesotho needs a legal framework for cyberstalking and revenge porn. Moreover, detecting cyber harassment and finding legal mechanisms to deter potential perpetrators, to find relevant means of investigating these cybercrimes and imposing appropriate punishments where the courts convict said perpetrators.

The overall aims of this study are twofold; firstly, it is to highlight and critically examine the current framework in as far as it may be relevant in terms of addressing cyber harassment with sexual nuances and secondly, it is to critically examine the relevant sections of the Computer Crimes and Cybercrimes Bill of 2020 to ascertain whether the relevant provisions are adequate for the effective regulation of cyber harassment, cyberstalking and revenge porn in Lesotho. This evaluation will rely on a framework that is based on the international human rights requirements for the protection of learners and people in the workplace, the current South African legal framework and examples from American law which will be fully dealt with in Chapter Three.

[19] https://www.unodc.org

In a nutshell, the objectives of this study are:

1. To examine Lesotho's current legal framework and identifying gaps that will bring Lesotho's law to par with other jurisdictions and eventually coming up with recommendations.
2. To critically examine the Computer Crimes and Cyber Security Bill of 2020 which is Lesotho's first comprehensive attempt to deal with all cybercrimes including cyber harassment, cyberstalking and revenge porn which are the subject of this dissertation.
3. To examine how, cyberstalking and revenge porn in other jurisdictions are regulated by law so that law-enforcement agencies in Lesotho can be sensitized on effectively implementing the relevant sections of the Computer Crimes and Cybercrimes Bill of 2020.
4. Lastly, discharging the above mandate will enable the researcher to formulate recommendations in the concluding chapter of this dissertation.

1.5. METHODOLOGY

The researcher has selected to use a combination of qualitative desktop research and qualitative interviews using a semi-structured interview questionnaire with a sample of relevant stakeholders. These include the Child and Gender Protection Unit which is a unit of the Lesotho Mounted Police Services and a Human Resources Manager.

This dissertation engages in the investigations of the laws that govern cyber harassment in South Africa and California in the United States of America that has laws that govern cyber harassment, revenge porn and cyberstalking. The researcher has chosen South Africa because Lesotho uses the South African precedent when deciding some cases and South Africa seems to be getting somewhere with its cyber harassment laws.

The United States of America has been chosen because California has comprehensive laws that govern different types of cyber harassment. These investigations of the laws that govern cyber harassment are conducted in order to help Lesotho to formulate its own laws on cyber harassment. The recent Lesotho Computer Crime and Cyber Security Bill of 2020 will serve as a basis for future recommendations. Relevant international conventions such as the African Union Convention on Cyber Security and Personal Data Protection, journals, law reports, law textbooks, articles written by scholars and professors will be referred to. Various statutes which include the Computer Crimes and Cyber Security Bill of 2020 and the Codes of Good Practice will also be the source of information in this dissertation.

1.6. HYPOTHESIS

First research hypothesis

It is hypothesized that, the training of all police officers in the cyber-crime department to be skilled in the field of cyber technology and security would help in tackling cyberaggression in Lesotho.

Hypothesis as a question

Would training all police officers in the cyber-crime department to be skilled in the field of cyber-technology and security help in tackling cyberaggression?

Second research hypothesis

It is hypothesized that enacting a statute that addresses cyberaggression laws of various forms with a sexual undercurrent would result in a not so difficult task of tackling cyber harassment, cyberstalking, and revenge porn in Lesotho.

Hypothesis as a question

The present study attempts to address a gap in cyber harassment laws with a sexual undercurrent by addressing the following research question:

Will the existence of a statute that addresses cyber aggression laws of various forms help in tackling cyber harassment, cyberstalking, and revenge porn in Lesotho?

1.7 SYNOPSIS OF SUBSEQUENT CHAPTERS

The dissertation will be divided into four chapters. Chapter one will be a brief overview of what the researcher proposes to do in the study. This chapter also states the main problem that the researcher seeks to address, and the researcher provides ideas on what could be done to solve this problem of cyber harassment. Questions pertaining to the legal framework of cyber harassment in Lesotho are also posed in this chapter. Chapter one includes definitions of the key terms in this dissertation, which are cyber harassment, cyberstalking, and revenge porn.

Chapter two will be an exploration of different legal issues involved with cyber harassment in the workplace and higher education institutes. Chapter two is all about the literature review on cyberaggression. The legal framework of other jurisdictions which are domestic framework, African Union**,** SADC, and global framework are examined in this chapter.

Chapter three is a comparative study between Lesotho and the Republic of South Africa. Punishment for cyber harassment in the workplace in Lesotho and South Africa are different, hence this chapter seeks to compare how cyber harassment in South Africa is punishable compared to Lesotho. The legal framework of the United States of America will also be examined in the comparative analysis. Case law on cyber harassment is also discussed in this chapter. Lastly the extent to which cyber harassment laws is applied in Lesotho is also examined.

Chapter four which is the last chapter, rounds up the discussion with findings, conclusions and consists of a compilation of recommendations that seek to guide us towards a solution.

CHAPTER 2: CYBER HARASSMENT IN THE WORKPLACE AND IN HIGHER EDUCATION INSTITUTIONS

2.1 INTRODUCTION

The first part of this chapter is a literature review of cyber harassment in higher learning institutions and the workplace. The second part of this chapter is a review and thorough analysis of the international, continental, regional, and domestic legal framework of these forms of cyber harassment.

2.2 LITERATURE REVIEW

Many scholars call for a development of cyberspace laws. Stein and Solange in their book are of the view that new interests developed on cyberspace may need the protection of substantive criminal law. They argue that there is a need for new protection by legislation through a treaty[20]. Marc Goodman also states that the vast majority of virtual crimes have real world victims. He concludes by saying: "Given the complexity of the issues involved, now is the time to begin thinking and responding to these concerns before the virtual crime wave spills over into the real world." [21]

Some recent studies focus on the problem of criminalizing revenge pornography. Attorney Marc Randazza, for instance, contends that one problem with criminal statutes targeting revenge porn is the vast volume of cases that would need to be filed to mitigate the problem. Another issue with criminalizing revenge porn is that the necessity for legislation could largely be avoided if people simply stopped voluntarily sending nude photos of themselves to others.[22]

[20] http://pircenter.org/kosdata/page_doc/p2732_1.pdf
[21] https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=should+legislature+interfere++in+cybercrime&btnG=#d=gs_qabs&u=%23p%3Dtty1W_z3Gl0J
[22] https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1570&context=iplj

Warren Chik in his article argues that cyberstalking is a social problem that requires a unique set of legal remedies in order for the law to be effective in preventing and removing it. He further contends that criminalizing cyberstalking can provide appropriate sanctions to deal with perpetrators.[23]

Some scholars like Izak Post in his article highlights that the fact that thirty nine states in America have recognized the importance of directly criminalizing cyber harassment is a large step in the right direction, however, those laws bring enforcement challenges. This scholar also perceives cyberstalking and cyber harassment to mean two different types of online behaviors[24]. In this dissertation however, Cyber harassment is a catch-all phrase for cyberstalking and revenge pornography because they are both forms of cyber harassment.

A few authors limit their research to focus on cyber harassment in the workplace only, whereas others also limit their research to focus on cyber harassment in higher learning institutions only. In an article written by Monica, cyber harassment is termed to mean cyber bullying, for that matter, that article focuses on cyberstalking in the workplace as a form of bullying.[25] Justin Vance in his article contends that when cyber-bullying occurs amongst adults it is known as cyber-harassment. He further stated that related literature including university policies and online teaching guides suggested there may be a cyber-harassment problem in online learning in higher education as well although no quantitative evidence currently exists.[26]

[23] https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=harassment+through+digital&oq=harassme#d=gs_qabs&u=%23p%3DBF7mMvmrad4J

[24] http://www.law.msu.edu/king/2012-2013/Post.pdf

[25] https://books.google.com/books?hl=en&lr=&id=OmkQBAAAQBAJ&oi=fnd&pg=PA248&dq=info:yZ55bdEjTTcJ:scholar.google.com/&ots=0WZjT_DL3K&sig=qplqWcLGYctFugg4gzk_2H5FOmg

[26] http://search.proquest.com/openview/b84464891c23ec6e40e5e123ef28327d/1?pq-origsite=gscholar&cbl=18750&diss=y

Recent work has begun to challenge this criterion and argue for a more varied approach to understanding the legal framework of cyberstalking and revenge pornography. Although many civil and criminal laws apply to revenge porn, some scholars argue that using those laws is often hindered by disinterested law enforcement and suggest that new criminal legislation is necessary to protect victims.[27]

Recent literature focuses on the trans-nationality of such a crime in which cyberstalking is considered as a trans-border crime, therefore, according to Dhillon, Challa and Smith, cyberstalking ignites jurisdictional issues as it is a cross-border crime.[28] These 3 abovementioned authors have only focused on the jurisdictional issues, they did not get in to detail about the legislation of such crimes.

On the other hand, many recent studies have focused on cyberstalking as a crime to be punished. Hamin and Rosli's research revealed that cyberstalking is perceived as a risk to be managed rather than a crime to be punished. This means that victims of such crime or risks are believed to be responsible for manufacturing such risk by having unlimited access to the internet and by over sharing personal information in social media applications. [29]

Apart from that, there are scholars who advocate for a great need for the legislature to interfere in curbing cyber harassment. Paul, Mark and Leroy illustrate in their article that a great deal of evidence is available to show that cyberstalking is a significant and growing problem.[30] This means there is a need for the interference of the legislature. For instance, Cyber Angels (a well-known internet safety

[27] Ibid (p3)
[28] https://www.cybercrimejournal.com/Hamin&RosliVol12Issue1IJCC2018.pdf
[29] https://www.cybercrimejournal.com/Hamin&RosliVol12Issue1IJCC2018.pdf
[30] http://irep.ntu.ac.uk/id/eprint/17988/1/185311_3014%20Griffiths%20Publisher.pdf

organization) receives about 500 complaints of cyberstalking each day, of which up to 100 represent legitimate cases.[31]

Given the recent spread of literature in this area, this is a key point in time to draw together the current knowledge regarding revenge pornography and non-consensual sharing of private sexual media.[32] In the U.S 29 papers discussing legal components of revenge pornography/non-consensual sharing discussed several challenges to enacting revenge porn legislation that is effective and that does not raise constitutional issues. For example, eight articles (seven from the U.S, one from multiple countries) discuss the issue of protection of freedom of speech/expression in developing legislation that addresses revenge pornography behaviors.

Daniel's article highlight the challenges of developing revenge pornography legislation that does not impinge on First Amendment rights in the U.S. Daniels questions whether recent amendments to legislation that deals with revenge pornography in California could face challenges in relation to the First Amendment[33]. Barmore proposes that any revenge pornography legislation may not affect freedom of speech protection, as the images could be considered obscene (and as such are not protected by the First Amendment).[3435]

[31] http://irep.ntu.ac.uk/id/eprint/17988/1/185311_3014%20Griffiths%20Publisher.pdf
[32] https://pdfs.semanticscholar.org/4a50/1cb2773226afd7e2009415eb30a0d9ab96dd.pdf
[33] Daniels, M. (2014). Chapters 859 & 863: Model revenge porn legislation or merely a work in progress? McGeorge Law Review, 46, 297-320.
[34] Barmore, C. (2015). Criminalization in context: Involuntariness, obscenity, and the first amendment. Stanford Law Review, 67, 447-478.
[35] https://pdfs.semanticscholar.org/4a50/1cb2773226afd7e2009415eb30a0d9ab96dd.pdf

In proposing solutions for revenge pornography victims, three papers by Cannon, [36] Cecil[37], Tungate,[38] discuss the challenges that face victims and legal professionals in seeking the permanent removal of images from revenge pornography websites. In the U.S, section 230 of the Communications Decency Act (CDA) provides a level of immunity from prosecution for the hosts of such sites under certain circumstances. For example, website operators are protected from prosecution when content is provided by third parties, as is usually the case in such sites. Cannon argues that the CDA should not protect hosts when they have purposefully aided the development of the material that is published on the website.[39]

Both Cecil and Tungate argue for amendments to the CDA to facilitate victims of revenge pornography submitting takedown notices, once they know that content has been uploaded to such websites. Both authors acknowledge that there are significant challenges to ensuring that a takedown notice is effective, particularly with the ease at which content can be spread to other websites. However, they consider that amendments to the CDA would at least provide victims with a formalized process through which some content could be removed.

In 2007, 'Mamotumi Maliehe submitted a dissertation titled Cybercrime legislation for Lesotho. Her paper advocates introducing cybercrime legislation in Lesotho. Cybercriminals can commit various illegal activities in cyberspace that few people even know exist. Lesotho's current criminal laws can hardly be enforced against

[36] Cannon, L. (2015). *Indecent communications: Revenge porn and congressional intent of §* 230(c). Tulane Law Review, 90, 471-493

[37] Cecil, A. L. (2014). *Taking back the internet: Imposing civil liability on interactive computer services in an attempt to provide an adequate remedy to victims of nonconsensual pornography*. Washington & Lee Law Review, 71, 2513-2556

[38] Tungate, A. (2014). *Bare necessities: The argument for a 'revenge porn' exception in section 230 immunity.* Information & Communications Technology Law, 23, 172-188.

[39] Cannon, L. (2015). *Indecent communications: Revenge porn and congressional intent of § 230(c*). Tulane Law Review, 90, 471-493.

cybercrime, as they do not clearly prohibit the crime. Therefore, her dissertation argues that Lesotho must adopt a comprehensive legal structure to deter and prosecute cybercrime. She is of a view that examining international and national approaches to cybercrime will provide guidance for an effective framework capable of addressing this 'new' crime. Maliehe's dissertation is focused on cybercrime in general, not on cyber harassment only.[40]

Conclusion

The key findings that are observed from this literature review are that research seems to be focusing on cyberstalking and revenge pornography separately. Cyber bullying and cyber harassment are used interchangeably in most researches. There seems to be no satisfying legal frame work for cyber harassment in most countries, hence most scholars are of the view that cyber harassment must be criminalized.

2.3. THE LEGAL FRAMEWORK OF OTHER JURISDICTIONS

2.3.1. Domestic framework

Lesotho has a proposed draft of Computer Crimes and Cyber Security Bill of 2020 which will have cyber and computer crime related offences punishable by law.[41] South Africa's private sector is already involved in the national cyber security policy,[42] while the government of Lesotho is yet to encourage the private sector to get involved in the national security cyber policy.

[40] Maliehe, M. 2007 "Cybercrime legislation for Lesotho" Dissertation
[41] Informative Newspaper 03-09 March 2020
[42] Government Gazette , 4 December 2015 No.39475

Further discussions on the Bill will be made on the legislative definitions as contained in the bill in chapter 3 and chapter 4 of this dissertation.

Related laws and Regulations

Human Rights Act 24 of 1983 [43] only protects cyber harassment to the extent that it safeguards the fundamental rights of the citizens of Lesotho. According to section 4(1) (g), every person in Lesotho is entitled, whatever his race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status to fundamental human rights and freedoms, that is to say, the right to respect for private and family life.

In Lesotho, section 104 of the Penal code[44] deems cyberaggression unlawful to the extent of unlawful publication. This section states that a person who, by print, writing, painting or effigy, or by any means otherwise than solely by gesture, spoken words or other sounds, unlawfully publishes any defamatory matter concerning another person, with intent to defame that other person, commits an offence of defamation.

Section 200 of the Labour Code Order No.24 of 1992 explains what sexual harassment is, but that definition does not include that sexual harassment may occur through cyberspace as cyber harassment. However, 2003 Codes of Good Practice try to give an employer direction as to how to deal with sexual harassment in the workplace.[45]

Section 59(1) (c) (i.v) of the Codes of Good Practice mentions one of the forms of sexual harassment as the display of sexually explicit pictures and objects. It has been

[43] Human Rights Act 24 of 1983
[44] Penal Code Act , 2010
[45] Lesotho Times News Paper, April 13, 2018

noted therefore that institutions of higher learning have no sexual harassment policies that regulate sexual offences, let alone cyber- harassment policies.[46]

Sexual Offences Act, 2003 defines a sexual act to mean exposure or display of the genital organs of one person to any other person. This definition can also amount to revenge porn to some extent, but revenge porn in different terms is defined in the Computer Crimes and Cyber Security Bill 2020. Section 3(1) of the Sexual Offences Act further states that a sexual act is prima facie unlawful if it takes place in any coercive circumstances.

For the purpose of this dissertation, coercive circumstances are defined in Part 1 Section 2 of the Sexual Offences Act. Section 2 (g) states that the complainant submits to or commits the sexual act by reason of having been induced, whether verbally or through conduct, by the perpetrator, or by some other person to the knowledge of the perpetrator, to believe that the perpetrator or the person with whom the sexual act is being committed is some other person. In identifying the shortcomings of this Act, the sexual offences does not show that sexual harassment can still occur through the cyber space.

The absence of sexual harassment policy has been blamed for the continuing violations of students' sexual rights. In order to address the gender gaps in the processes, practices and the curriculum at the National university of Lesotho, a Gender Action Plan has been developed under the auspices of Commonwealth of Learning.[47]

However, this country has a "Lesotho ICT Policy 2005." [48] This policy was created to fulfill the goals set out in the Lesotho vision 2020 Policy document as well as the

[46] Ntho. Mamoeketsi, March 2013 "A review of AfriMAP and the Open Society Initiative for Southern Africa"
[47] www.nul.ls /nul-hosts-gender-dialogue/
[48] ICT Policy for Lesotho, Final. 4 March 2005

Poverty Reduction Strategy Paper, and supersedes the Lesotho Telecommunications Policy of 1999. [49] While the ICT policy does not contain any provision that deal specifically with cybercrime, it provides for the enabling of an ICT legislative and regulatory framework for various sectors such as e-commerce and health.

Lesotho has the added advantage of learning and borrowing from the experiences of her sister countries such as the United Kingdom, the United States of America and South Africa that have already enacted cyber harassment laws.[50]

2.3.2. African Union

The African Union Convention on Cyber Security and Personal Data Protection [51] has been enacted to establish a legal framework for cyber-security and personal data protection which embodies the existing commitments of African Union member states at sub-regional, regional and international levels to build the information society.

Article 13, principle 2 of the African Union Convention on Cyber Security and Personal Data Protection provides for the lawfulness and fairness of personal data processing. It states that the collection, recording, processing and transmission of personal data shall be undertaken lawfully, fairly and non-fraudulently. For the purposes of this dissertation, cyber harassment in the form of revenge porn amounts to transmission of personal data unlawfully.

Unfortunately, Lesotho is one of the many other countries that have not signed, ratified/acceded to the African Union Convention on Cyber Security and Personal

[49] The Lesotho Telecommunications of 1999

[50] Maliehe, M. 2007 "Cybercrime legislation for Lesotho" Dissertation

[51] The African Union Convention on Cyber Security and Personal Data Protection Adopted by the twenty –third ordinary session of the assembly, held in Malabo, Equatorial Guinea

Data Protection. In order for this convention to apply in Lesotho, Lesotho must sign and ratify the African Union Convention on Cyber Security.[52]

2.3.3. SADC

The SADC model law on computer crime and cybercrime provides for the harmonization of SADC region country policies towards cybercrime by primarily identifying cybercrime offences. Lesotho is yet to create legislation on cybercrime, it only has a Bill so far.[53]

2.3.4. Global framework

The UN has long been a leader in addressing global issues and has engaged in multiple efforts relating to cybercrime. Various bodies within the UN have initiated significant research and negotiations to reach a consensus on a number of cyberspace issues, including setting standards on providing security for networks, and establishing a forum on challenging issues, such as spam and information security.[54]

In 1990, the Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders addressed the legal challenges of cybercrime.[55] The Congress produced a resolution calling for Member States to intensify efforts in combating computer crime, by improving computer security and preventive measures, and promoting the development of a comprehensive international framework of guidelines and standards addressing future computer-related crimes. Most particularly, the resolution calls for Member States to intensify efforts in modernizing national criminal laws and procedures, including measures to: ensure that existing offences

[52] https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/lesotho/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=fi_FI

[53] Ibid(p8)

[54] Maliehe, M. (2007) *Cybercrime Legislation For Lesotho* Dissertation

[55] Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.'

and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and, if necessary, make appropriate changes.[56]

In 1994, the UN Manual on the Prevention and Control of Computer-Related Crime was published. The Manual examines the phenomenon of computer crime, substantive criminal law protecting the holder of data and information, substantive criminal law protecting privacy, human rights, procedural law, crime prevention in the computer environment, and the need for developing international co-operation.[57]

Article 4(1) of the Convention Concerning the Elimination of Violence in the World of Work [58] states that each Member which ratifies this Convention shall respect, promote, and realize the right of everyone to a world of work free from violence and harassment. Unfortunately, Lesotho has not ratified this convention.

2.4. Conclusion

This chapter has examined the legal frameworks and the two forms of cyber harassment that take place in the workplace and in higher education institutions. In identifying the gaps in terms of the domestic framework, Lesotho has laws that are close to addressing cyber harassment, unfortunately they are not specific. The two forms of cyber harassment outlined in this chapter occur in Lesotho but there is no precedent and legislation on them. Lesotho can intelligently borrow from external initiatives to enact a comprehensive legal structure to combat cybercrime especially of the variety that promotes gender-based violence.

[56] Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.
[57] UN Manual, Note 184
[58] Convention Concerning the Elimination of Violence and Harassment in the World of Work, adopted by the Conference at its 108th session, Geneva, 21 June 2019.

CHAPTER 3: COMPARATIVE STUDY

3.1. INTRODUCTION

This chapter addresses the Lesotho Computer Crime and Cyber Security Bill of 2020 together with its shortcomings. This chapter will also analyse the relevant cybercrime laws of South Africa and the United States of America and evaluate our Computer Crime and Cyber Security Bill in light of the regional and international trends elicited herein.

3.2. LEGAL FRAMEWORK OF WORKPLACE CYBER HARASMENT IN LESOTHO COMPARED TO SOUTH AFRICA

Lesotho's current criminal laws can hardly be enforced against cybercrime, as they do not clearly prohibit the crime.[59] South Africa regulates cybercrime related to revenge porn and cyberstalking under:

- The Films and Publications Act 65 of 1996 as amended by the Films and Publications Amendment Act 34 of 1999 and Act 18 of 2004. This Act provides for the classification of certain films and publication not suitable for persons below 18 years of age and for the registration of Internet service providers, obliging service providers to take reasonable steps to prevent distributing child pornography.[60] Further, this Act prohibits possessing, producing, procuring, accessing and distributing child pornography and distributing restricted harmful material.[61] This also covers activities committed over the Internet.[62]

[59] Maliehe, M. 2007, *Dissertation on Cybercrime Legislation for Lesotho.*
[60] Sections 2 and 27A
[61] Films and Publication Act Sections 27 and 28
[62] Films and Publication Act Section 2(a) (I).

Thus, anyone possessing, producing, accessing and distributing child pornography, distributing restricted harmful material and not meeting the Internet service providers' obligations commits an offence.[63] Conviction for this offence is a fine, or imprisonment for not more than ten years, or both.[64]

- Cybercrime related to revenge porn in South Africa is also regulated by the Copyright Act 98 of 1978 as amended by the Copyright Amendment Act 56 of 1980, 66 of 1983, 52 of 1984, 39 of 1986, 13 of 1988, 61 of 1989, 125 of 1992, the Intellectual Property Amendment Laws 38 of 1997 and the Copyright Amendment Act of 9 of 2002. Lesotho's copyright law does not address offences committed by electronic means.
- The Protection from Harassment Act 17 of 2011 [65] came into effect on 27 April 2013. The Protection from Harassment Act provides for an inexpensive civil remedy in instances of cyber harassment and provides recourse for both domestic and non-domestic relationships. The definition of 'harassment in section 1 of the abovementioned Act broadly includes, cyberstalking and electronic communications that may be harmful.[66]

  The legislature in enacting the Protection from Harassment Act attempted to rectify the shortcomings of the Domestic Violence Act. It did this by bringing the perpetrators of cyber harassment to justice by including provisions that enable a complainant being cyber harassed to obtain the required evidence that can allow for positive identification of a perpetrator. For instance, section 4 of the Protection from Harassment Act places an obligation on Internet Service Providers to aid law enforcement by providing any information to

[63] Films and Publication Act Sections 27, 27A and 28
[64] Films and Publication Act Sections 30(1) and (1A).
[65] The Protection from Harassment Act 17 of 2011
[66] www.derebus.org.za/are-your-hands-tied-when-it-comes-to-cyber-harassment/

ascertain the identity of the perpetrator within 5 days of having been served with a request for same from law enforcement.[67]

President Cyril Ramaphosa signed several new bills into the South African Law in 2019, one of them is the amendments made to the Films and Publications Bill. As well as clamping down on hate speech and the sharing of child pornography, laws prohibiting the distribution of revenge porn have been ratified.[68]

The new laws take these offences extremely seriously. An individual can now be jailed for:

- Knowingly distributing private sexual photographs or films without the prior consent of an individual featured.
- Sharing these types of photos publicly with the intention to cause harm or distress.
- Uploading private sexual photographs where the person can be clearly identified or is named in any accompanying text.

If an individual is found guilty of contravening this amended bill, they suffer serious consequences. Basic offences come with a maximum jail sentence of two years, and a fine rising to R150 000. However, if one posts revenge which identifies the victim, both the prison time (four years) and the financial penalty (R300 000) double-up.

3.3. LEGAL FRAMEWORK OF WORKPLACE CYBER HARASMENT IN THE UNITED STATES OF AMERICA

Generally, the United States has comprehensive legislation governing cyber harassment. However, this dissertation is going to focus on only one state in America, which is California. The Penal Code 647j PC is the California statute that

[67] www.derebus.org.za/are-your-hands-tied-when-it-comes-to-cyber-harassment/
[68] Head, T. 2019. "South Africa's new "revenge porn" laws: here's what will land you in jail."

makes it a crime for a person to engage in revenge porn. This statute applies to the situation where:

1. A 'victim' initially consents to the recording of sexual images of him/her
2. She/he has the understanding that the images will remain private.
3. The defendant distributes those images without the consent of the owner of the images.

According to the legal framework of California, the defendant can raise defences. These defences are:

1. No intentional distribution
2. No intent to cause emotional distress and /or
3. Consent.

There are also penalties for this offence. The crime of revenge porn is a California misdemeanor. This is opposed to a felony or an infraction. This offence is punishable by:

I. Custody in country jail for up to six months, and/or
II. A maximum fine for $1, 000.

In addition to the abovementioned statute, California has an Assembly Bill 602[69] which is a relatively new piece of California legislation. If this Bill is approved, it will give the victims of fake sexual videos the right to sue the person who created it or shared it.[70] For laws that regulate cyberstalking in California, the Penal Code section 646.9 [71] is used.

[69] California Assembly Bill 602
[70] https://www.shouselaw.com/revenge-porn.html
[71] California Penal Code Section 646.9

3.4. CASE LAW ON WORKPLACE VIOLENCE AND HIGHER EDUCATION INSTITUTIONS

In S v Trainor[72] the court held that evidence, of course, must be evaluated against the onus of any particular issue or in respect of the case in its entirety. 'Onus in harassment cases conducted electronically or otherwise, is on the complainant to show that they are entitled to protection against the perpetrator because the perpetrator's conduct constitutes harassment in terms of the Domestic Violence Act 116 of 1998 [73] or any other legislation.

A Delaware attorney who interviewed prospective students for his alma mater law school became the victim of a relentless campaign of online harassment by a prospective student who did not get into the school. The prospective student, Yung, cyber harassed the victim and his family by cyber stalking him. Yung pleaded guilty to cyberstalking charges in October 2018. In February 2019, he was sentenced to 46 months in prison.[74] This case demonstrates that cyberstalking can also take place in higher learning institutions.

Nearly two dozen times, Francesca Rossi called law enforcement to complain that an ex- partner was harassing her online, posting nude images of her and the like. But they could not make it stop and could not even make an arrest for almost a year, until the man set off a national panic by posing as Rossi to make bomb threats against Jewish centers across the country. That turned it into a major federal case that ended with her tormentor, Juan Thompson being arrested within a few days and eventually sentenced to five years in prison.[75]

[72] 2003(1) SACR 35 (SCA) AT PARA 9
[73] Domestic Violence Act 116 of 1998
[74] https://www.fbi.gov/news/stories/cyberstalker-sentenced-061019
[75] https://www.seattletimes.com/nation-world/cyberstalking-victim-says-she-feared-tormentor-would-kill-her/

In the case of United States v. Coss[76] the defendants created two fictitious personas, used for communications in which the perpetrators claimed to be a seventeen-year-old girl, impregnated by the recipient of the communication. The defendants claimed to have compromising photographs and threatened to sell those photos to a tabloid unless the victim purchased the photographs.

United States v. Shrader[77] explains that stalking may consist of many separate acts which cumulatively cause the victim great emotional distress. In the case of People v. Costales[78] the victim, a musician, had an "an open profile" Myspace account used to market her music, on which the defendant posted sexually suggestive messages.

In the case of United States v. Savader[79] by hacking the victims' online accounts, the defendant "obtained compromising photos of the victims," which "would be shared with parents, employers, boyfriends or other members of the community unless the perpetrator's demands were met.

In United States v. Sayer[80] the defendant posted video clips of his ex-partner on adult pornography websites, depicting sexual acts performed by the victim during their relationship, along with the victim's name and address. The defendant also created fictitious online advertisements and social media profiles with the victim's name, through which men were invited "to come to her home for sexual encounters." Following those postings, a plethora of men reached the victim's location, seeking sexual encounters, terrifying the victim, and instilling the fear that she would be raped or assaulted.

[76] 677 F.3d 278, 281 (6th Cir. 2012)
[77] 675 F.3d 300, 311-12 (4th Cir. 2012)
[78] 2d Crim. No. B215915, 2010 WL 2044637, at *1-2
[79] 944 F. Supp. 2d 209, 210 (E.D.N.Y. 2013)
[80] 64 No. 2:11-CR-113-DBH, 2012 WL 1714746 (D. Me. May 15, 2012).

In the case of People v. Rosa[81] after their approximately ten-year marriage ended, the defendant threatened to kill the victim claiming he would, "put a bullet between her eyes." The defendant also placed nude photographs of his former wife online, taken during their marriage, and advertisements that the victim was keen to meet men and perform oral sex. As a result of the postings, the victim received numerous phone calls and visits at her workplace from men inquiring about the ads.

3.5. CRITICAL EXAMINATION OF THE COMPUTER CRIMES AND CYBER SECURITY BILL OF 2020

Part 1 of the Computer Crimes and Cyber Security Bill does not have the definition of cyberstalking, cyber harassment, and revenge pornography, it only has the definition of cybersquatting and other cybercrimes. For a bill that deals with computer crimes and cyber security to not have the definitions of the most important computer crimes constitutes a very huge gap in the legislature.

Section 15(1) of the Bill is about the distribution of data messages of intimate images without consent. This section creates an offence for any person who unlawfully and intentionally makes available, broadcasts or distributes, by means of a computer system, a data message of an intimate image of an identifiable person knowing that the person depicted in the image did not give his or her consent to the making available, broadcasting or distribution of the data messages commits an offence and is liable, on conviction, to a fine not exceeding M40,000 or imprisonment for a term not exceeding five years, or both.

This statute does not come to terms with using modern terminology. The offence described in section 15(1) is normally termed as revenge pornography, otherwise known as image-based sexual abuse. From the onset this statute has not defined what

[81] No. F063748, 2013 WL 941728 (Cal. Ct. App. Mar. 12, 2013).

image based sexual abuse is. The offence on its own is clear, that the distribution of such intimate images must be of an identifiable person, the distribution must also be without consent.

Section 22(1) of the abovementioned bill is about harassment or cyber-bullying using means of electronic communications. Cyber-stalking and revenge-porn can amount to cyber-bullying according to this Bill. This section reads as follows:

A person who intentionally, without lawful excuse or justification, or in excess of a lawful excuse or justification-

a) initiates any electronic communication, with the intent to coerce, intimidate, harass, abuse, or cause substantial emotional distress to a person; or
b) initiates offensive and obscene communication with the intent to disturb the peace, quiet and privacy of another person, whether or not a conversation ensues,

commits an offence and is liable, on conviction, to imprisonment for a term not exceeding ten years, or a fine of not exceeding M100, 000 or both.

Section 22(2) of the Computer Crimes and Cyber Security Bill further goes on to say that a person who intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification initiates any electronic communication or uses a computer system with the intent to support severe, repeated and hostile behavior, commits an offence and is liable, on conviction, to imprisonment for a term not exceeding ten years, or a fine not exceeding M100, 000 or both.
In this instance, if stalking is done repeatedly online, then the perpetrator has violated this section.

Since cyber- harassment can occur through computer systems of institutions like a business or a school, section 35(1) of the Bill states the obligation of institutions.

Sub-section (1) (a) says that an institution that becomes aware that its computer system is involved in the commission of any offence under this Act shall-

a) report the offence to the law enforcement authorities within a period of not later than 24 hours; and
b) preserve any information which the law enforcement authorities may require for the investigation of the offence.

(2) An institution which fails to comply with this section is guilty of an offence and shall, on conviction, be liable to a fine not exceeding M250, 000.

Section 39(1) of the Bill provides for the jurisdiction. It says that a court in Lesotho shall have jurisdiction to try any offence under this Act where the offence has been committed wholly or in part.

3.6. CONCLUSION

Lesotho can borrow from South Africa and the United States of America to enact a comprehensive legal structure to combat cybercrime as these states have comprehensive laws on cyber-harassment. This chapter has highlighted that there is little case law on cyber harassment. Lesotho on the other hand does not have cases on cyber harassment at all.

CHAPTER 4: CONCLUSION AND RECOMMENDATIONS

4.1. INTRODUCTION

This chapter is an overview of all the chapters of this dissertation and its results. Not much has been written pertaining to the plea for the legislature to interfere with the laws governing cyber aggression in Lesotho. The current chapter is the last chapter which will also provide a conclusion, findings and also recommendations because at the end there has to be clarity in what the dissertation has addressed. The findings that will be provided for are the findings that resulted from the interviews and the research from articles and books. For this dissertation to be purposeful, clear recommendations are to be provided for to enable the legislature of Lesotho to enact laws that will address the cyber harassment problem in Lesotho.

4.2. FINDINGS

The findings section of this dissertation serves the purpose of presenting the key results and important data that was collected during this research.[82] The statement of the problem in chapter 1 of this dissertation was that the problem with Lesotho's government is that it has only drafted a Bill on Computer Crimes and Cyber Security of 2020 which is not yet enforceable because it is not an Act. It has been established that some stake holders are aware of the Computer Crimes and Cyber Security Bill of 2020 while some are not aware of it.

The second problem was that there is very little or no jurisprudence/ case law on cyber harassment in Lesotho. The interview conducted between the researcher and the Child and Gender protection Unit was helpful to some extent in that the researcher got to know that cyberstalking and revenge porn do take place in Lesotho

[82] https://www.researchprospect.com/how-to-write-the-findings-of-a-dissertation/

but the law enforcement agencies cannot do anything about it because there is no law on cyber harassment in Lesotho yet. One of the overall aims of this study was to firstly, highlight and critically examine the current framework in as far as it may be relevant in terms of addressing cyber harassment with sexual nuances. In critically examining Lesotho's current legal framework, it was discovered that it was inadequate, and it is still inadequate. Secondly the aim of this dissertation was to critically examine the relevant sections of the Computer Crimes and Cybercrimes Bill of 2020 to ascertain whether the relevant provisions are adequate for the effective regulation of cyber harassment, cyberstalking, and revenge porn in Lesotho. As a result of this critical examination, the researcher found that the statute lacks definitions of some of the key terms of cyber harassment.

This dissertation also examined how, cyberstalking and revenge porn in other jurisdictions are regulated by law and Lesotho seems to be not in par with other jurisdictions. It was hypothesized that the existence of a statute that addresses cyber aggression of various forms would help in tackling cyber harassment, cyberstalking, and revenge porn in Lesotho. Since there is no statute on cyber harassment in Lesotho, cyber harassment cases cannot be dealt with by law enforcement agencies, especially the police.

4.3. CONCLUSION

It is evident from this dissertation that there is lack of cyber harassment research in Lesotho. There is either little to no focused research within the cyber security space in Lesotho. Lesotho is more vulnerable to most cyber harassment as there is no knowledge on cyber harassment despite increasing rate of internet usage. The overall present understanding of cyber harassment is inadequate in Lesotho, therefore providing nationwide awareness about cybercrime in Lesotho is necessary.

There is also lack of cyber harassment awareness. Many people, young and old, in the workplace and in higher learning institutions are victims to cyberstalking and revenge pornography due to their lack of awareness therefore resulting to non-reporting of such crimes. Technology is being adopted by many citizens in developing countries. The need for cyber harassment protection with sexual nuances within the workplace and higher education institutes is undisputable because this is a growing problem. The research conducted through this paper concludes that cyber harassment laws must be included in the workplace policies and higher education institution polices. Thus, this dissertation concludes that developing countries such as Lesotho will benefit from the development and adoption of laws that will protect cyberstalking and revenge pornography.

4.4. RECOMMENDATIONS

Recommendations could be made that users should change their passwords regularly or use fingerprints as their passwords. This will ensure that other individuals do not get access to computers or cellphones with intimate pictures that can be used as a source of revenge pornography.

Lesotho needs to pass an Act of parliament as soon as possible because the Computer Crimes and Cyber Security Bill has already been drafted. It is also recommended that the Computer Crimes and Security Bill must include definitions of cyberstalking and revenge pornography respectively. Lesotho must also amend the Labour Code Order, Codes of Good Practice, Sexual Offences Act and the Penal Code Act to encompass the use of computer technology in committing conventional offences. Lesotho must enact a statute that addresses cyberaggression laws of various forms with a sexual undercurrent.

1. Rules and regulations in higher learning institutions.

Each and every tertiary and other higher learning institutions must have rules and regulations that govern cyber-harassment amongst students as each and every student is exposed to the likelihood of being victims of cyber-harassment because of use of the internet.

2. Educating about cybercrime

Every workplace must educate and carry out training programs frequently as technology evolves gradually. This is to enable people in the workplace to stay alert and know when to report such cybercrimes, specifically cyber-harassment. In educating employees in the workplace about cyber-harassment, employers must also adopt cyber-harassment policies, which will also include cyberstalking and revenge pornography. These are very serious crimes that can render an employee or employer to lose their jobs, hence educating them frequently is very important.

There has to be leading organizations, public or private, taking the responsibility of making people aware of the cyberaggression issues that Lesotho faces. It is therefore important to have different cyber prevention aspects and integrate them into a multi-dimensional implementation plan, in the quest to raise and promote cyber safety, cyber awareness, capacity building, research and development and assist developing countries in promoting a cybersecurity culture.[83]

Largely, the Convention on Cybercrime has shaped the model law for cybercrime legislation for Lesotho. Although Lesotho is not a member, fully associating with the Convention would be a step in the right direction with regard to combating cybercrime. Further, Lesotho would better prepare for the Convention by

[83] N. N. Mosola, K. F. Moeketsi et al. *Cybersecurity Protection Structures: The Case of Lesotho.* World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering Vol:13, No:3, 2019

incorporating it into her own legislation, thus addressing her domestic issues before attempting the international. Meanwhile, Lesotho should consider signing and ratifying the Convention.[84] According to South African law, in instances where there is a lack of law in a specific area, reference to international jurisdictions is permissible.[85]

The researcher recommends that when Lesotho is faced with cyber harassment cases, it must also make reference to international laws. The training of all police officers in the cyber-crime department to be skilled in the field of cyber technology and security would help in tackling cyberaggression in Lesotho, therefore Lesotho must train law enforcement agencies such as the police in the use of computers. The Computer Crimes and Cyber Security Bill serves as a basis for future recommendations that it must be used to combat cyber harassment in the workplace and higher education institutes in Lesotho.

3. Reporting requirements

Lesotho must consider making a reporting requirement for cybercrimes. Cybercrime victims, particularly companies, tend to hide cybercrime attacks because they fear negative publicity and lack faith in the law machinery. A reporting requirement will assist in investigating and prosecuting a greater number of cybercriminals[86]. Additionally, future cybercrime incidents may be reduced as more prosecutions are publicized.[87]

[84] Maliehe, M. 2007 *Dissertation on Cybercrime Legislation For Lesotho*
[85] Reinhardt Buys (ed) Cyberlaw @ SA Top 100 FAQs Virtual Book 294
[86] Jason Chang 'Computer hacking: making the case for a national reporting requirement' (April 2004) Berkman Center for Internet & Society at Harvard Law School Research Publication No. 200407. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=530825 [Accessed 9 January 2007].
[87] ibid

4. The Courts of Lesotho

Our courts in this country must decide cyber harassment cases so that precedent shall be used in deciding cases that will be used in deciding cases that will come up afterwards. The courts of Lesotho must decide such cases basing themselves on S.A statutory law or common law.

5. Using intellectual property rights to combat revenge pornography.[88]

Copyright law may provide a tool for victims to expediently remove their sexually explicit images from the web.[89] By registering their intimate pictures through the Industrial Property Order No.5 of 1989 Lesotho, victims of revenge pornography in Lesotho may get to remove their images from the web.

[88] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2374119.
[89] https://www.cippmcgill.ca/news/2016/12/20/using-copyright-law-to-fight-revenge-porn/

BIBLIOGRAPHY

Books and Articles

1. Barmore, C. (2015). Criminalization in context: Involuntariness, obscenity, and the first amendment. Stanford Law Review, 67, 447-478.
2. Budde, R. (2014). taking the sting out of revenge porn: Using criminal statutes to safeguard sexual autonomy in the digital age. Georgetown Journal of Gender and the Law, Forthcoming.
3. Cannon, L. (2015). *Indecent communications: Revenge porn and congressional intent of §* 230(c). Tulane Law Review, 90, 471-493
4. Cecil, A. L. (2014). *Taking back the internet: Imposing civil liability on interactive computer services in an attempt to provide an adequate remedy to victims of nonconsensual pornography*. Washington & Lee Law Review, 71, 2513-2556
5. Citron DK, Franks MA. (2014). "Criminalizing revenge porn. Wake Forest Law Rev. 49,345-391.
6. Daniels, M. (2014). Chapters 859 & 863: Model revenge porn legislation or merely a work in progress? McGeorge Law Review, 46, 297-320.
7. Drebing H, Bailer J, ET al. (2014) "Cyberstalking in a sample of social network users: Prevalence, characteristics, and impact upon victims. Cyberpsychol Behav Soc Netw. 17, 61-67
8. Head. T. (2019). "South Africa's New "Revenge Porn" laws: Here's What Will Land You In Jail."
9. Informative Newspaper 03-09 March 2020
10. Jason Chang 'Computer hacking: making the case for a national reporting requirement' (April 2004) Berkman Center for Internet & Society at Harvard Law School Research Publication No. 200407. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=530825 [Accessed 9 January 2007].
11. Lekena, M. "An Exploration of Learners' Experiences of Bullying As An Act That Promotes Exclusion in a High School in Botha-Bothe District, Lesotho (Master of Education, Faculty of Humanities)
12. Lesotho Times News Paper, April 13, 2018
13. Maliehe, M. (2007) *Dissertation on Cybercrime Legislation For Lesotho*
14. Michael L. Pittaro, (2007) "Cyber stalking: An Analysis of Online Harassment and Intimidation."
15. N. N. Mosola, K. F. Moeketsi et al. *Cybersecurity Protection Structures: The Case of Lesotho.* World Academy of Science, Engineering and

Technology International Journal of Computer and Information Engineering Vol:13, No:3, 2019
16. Ntho, M. March (2013) "A Review of AfriMAP and the Open Society Initiative for Southern Africa"
17. Petrocelli, J. (2005). Cyber stalking. Law & Order, 53(12), 56-58
18. Prof Davidson. J, et al, (2019). Adult Online Hate, Harassment and Abuse "*A rapid evidence assessment*"
19. Reinhardt Buys (ed) Cyber Law @ SA Top 100 FAQs Virtual Book 294
20. Reno, J. (1999). 1999 report on cyber stalking: A new challenge for law enforcement and industry. Retrieved Feb. 18, 2006, from United States Department of Justice Web site: http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm
21. Tungate, A. (2014). *Bare necessities: The argument for a 'revenge porn' exception in section 230 immunity.* Information & Communications Technology Law, 23, 172-188.
22. Young. B, *Introduction to Qualitative Research Methods*, University of Liverpool.

Websites

1. https://www.fbi.gov/news/stories/cyberstalker-sentenced-061019
2. www.nul.ls /nul-hosts-gender-dialogue/
3. https://www.seattletimes.com/nation-world/cyberstalking-victim-says-she-feared-tormentor-would-kill-her/
4. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2374119.
5. https://www.cippmcgill.ca/news/2016/12/20/using-copyright-law-to-fight-revenge-porn/
6. https://www.researchprospect.com/how-to-write-the-findings-of-a-dissertation/
7. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=harassment+through+digital&oq=harassme#d=gs_qabs&u=%23p%3DBF7mMvmrad4J
8. http://www.law.msu.edu/king/2012-2013/Post.pdf
9. https://books.google.com/books?hl=en&lr=&id=OmkQBAAAQBAJ&oi=fnd&pg=PA248&dq=info:yZ55bdEjTTcJ:scholar.google.com/&ots=0WZjT_DL3K&sig=qplqWcLGYctFugg4gzk_2H5FOmg

10. http://search.proquest.com/openview/b84464891c23ec6e40e5e123ef28327d/1?pq-origsite=gscholar&cbl=18750&diss=y
11. https://www.cybercrimejournal.com/Hamin&RosliVol12Issue1IJCC2018.pdf

12. https://www.cybercrimejournal.com/Hamin&RosliVol12Issue1IJCC2018.pdf
13. http://irep.ntu.ac.uk/id/eprint/17988/1/185311_3014%20Griffiths%20Publisher.pdf
14. http://pircenter.org/kosdata/page_doc/p2732_1.pdf
15. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=should+legislature+interfere++in+cybercrime&btnG=#d=gs_qabs&u=%23p%3Dtty1W_z3Gl0J
16. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1570&context=iplj
17. https://definitions.uslegal.com/c/cyber-harassment/
18. https://www.cybercrimejournal.com/pittaroijccvol1is2.htm
19. http://irep.ntu.ac.uk/id/eprint/17988/1/185311_3014%20Griffiths%20Publisher.pdf
20. https://pdfs.semanticscholar.org/4a50/1cb2773226afd7e2009415eb30a0d9ab96dd.pdf
21. https://www.shouselaw.com/revenge-porn.html
22. https://www.unodc.org
23. www.derebus.org.za/are-your-hands-tied-when-it-comes-to-cyber-harassment/
24. https://www.coe.int/en/web/octopus/country-wiki/ /asset_publisher/hFPA5fbKjyCJ/content/lesotho/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=fi_FI

Statutes

1. California Assembly Bill 602
2. California Penal Code Section 646.9
3. Children's Protection and Welfare Act 2011 Act No.7
4. Labour Codes of Good Practice Notice 2003
5. Computer Crimes and Cyber Security Bill 2020

6. Convention Concerning the Elimination of Violence and Harassment in the World of Work, adopted by the Conference at its 108th session, Geneva, 21 June 2019.
7. Domestic Violence Act 116 of 1998
8. Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.
9. Films and Publication Act.
10. Government Gazette, 4 December 2015 No. 39475
11. Human Rights Act 24 of 1983
12. ICT Policy for Lesotho, Final. 4 March 2005
13. Lesotho Labour Code Order, No.24 of 1992
14. Penal Code Act 2010
15. Sexual Offences Act 2003
16. The Protection from Harassment Act 17 of 2011
17. The Lesotho Telecommunications of 1999
18. The African Union Convention on Cyber Security and Personal Data Protection Adopted by the twenty –third ordinary session of the assembly, held in Malabo, Equatorial Guinea
19. UN Manual, Note 184

List of cases

1. People v. Costales, 2d Crim. No. B215915, 2010 WL 2044637, at *1-2
2. People v. Rosa No. F063748, 2013 WL 941728 (Cal. Ct. App. Mar. 12, 2013).
3. S v Trainor 2003(1) SACR 35 (SCA) AT PARA 9
4. United States v. Coss 677 F.3d 278, 281 (6th Cir. 2012)
5. United States v. Shrader 675 F.3d 300, 311-12 (4th Cir. 2012)
6. United States v. Savader 944 F. Supp. 2d 209, 210 (E.D.N.Y. 2013)
7. United States v. Sayer 64 No. 2:11-CR-113-DBH, 2012 WL 1714746 (D. Me. May 15, 2012)