

UNIVERSITY OF KWAZULU-NATAL
FACULTY OF LAW AND MANAGEMENT STUDIES
SCHOOL OF LAW, HOWARD COLLEGE

A Critical Review of South Africa's Response to Cybercrime forms of Gender-Based Violence.

Research dissertation submitted by: Suhail Jadwat (218006111)

Supervisor: *Dr J L Hicks*

Co-supervisor: *Ms SP Jali*

DECLARATION REGARDING ORIGINALITY

I Suhail Jadwat.declare that:

A. The research reported in this dissertation, except where otherwise indicated, is my original research.

B. This dissertation has not been submitted for any degree or examination at any other university.

C. This dissertation does not contain any other persons' data, pictures, graphs or other information, unless specifically acknowledged as being sourced from such other persons.

D. This dissertation does not contain other persons' writing or ideas unless specifically acknowledged as being sourced from such persons. Where other written sources have been used then:

   - Ideas from such sources have been summarised in the present author's words, but the ideas have been attributed to such sources, which have been referenced.
   - Where exact words from these sources have been used, these words have been placed inside quotation marks, and referenced.

E. Where I have reproduced a part of a publication of which I am an author, co-author or editor, I have indicated in detail whether that part of the publication was written by myself alone, or by myself together with others and I have fully referenced such publications.

F. This dissertation does not contain text, graphics or tables copied and pasted from the internet, unless specifically acknowledged, and the sources detailed in the body and/or reference section of this dissertation.

Signed: *Suhail Jadwat*

Date: 24 April 2024

ACKNOWLEDGEMENTS

I wish to express my gratitude to my supervisors, Dr Hicks and Ms Jali, for their willingness to support me throughout this journey and for their unwavering patience, invaluable guidance and immense motivation and support and assistance at any time. This is a topic that I have been passionate about, and I am always grateful that together we were able to bring it to life.

I wish to thank my parents, Sabiha Jadwat and Ismail Jadwat, who have always been the rock and support in my life, who I absolutely owe everything to, who believed in me, and who supported me throughout everything. A special thank you goes to my mother, Sabiha Jadwat, who is my biggest cheerleader and has sacrificed everything for me; I am always grateful andlove you.

A special thank you goes to Sarah Jadwat, who has been with me throughout the journey, is my rock, stands with me through thick and thin, and supports me through everything. Your constant support and belief in seeing me succeed allow me to push through daily. A special thank you to Uncle Ak and Aunty Zeenath, Ahmed and Ayesha, your prayers and always being there for me mean a lot to me

This is a special mention for my uncle Yusuf Jadwat and my Nani and Papa and Dadi and Dada for all the sacrifices they had made so that I could pursue my dreams. I also would like to thank my immediate family members, my cousin's Saturday group, Dubai and Joburg cousins, my Gorikala and Masajee and my brother Johar for all their love and support.

Lastly, this idea was born during my schooling time, and I hope this dissertation serves as a voice for the voiceless that help is always out there and we are not alone, and it gives individuals the strength to continue and fight against these types of incidents.

ABSTRACT

This study critically evaluates South Africa's response to cybercrime forms of GBV, with the aim to contribute significantly to the existing literature. Through an analysis of legislative frameworks governing cybercrime-related GBV, the study identified implementation challenges thereby, providing insights for policymakers and law enforcement agencies. Additionally, the study assesses South Africa''s compliance with international law provisions regarding cybercrime and GBV, highlighting areas for improvement to align with global standards. The findings underscore the urgent need for cybersecurity awareness and training initiatives within South Africa, given the increasing internet penetration and susceptibility to cybercrimes targeting especially women. Despite recognising the intersection between GBV and technology, challenges persist in addressing emerging forms of gender-based cybercrimes. Recommendations are proposed to enhance law enforcement competency, empower women, eliminate cybercrime safe-havens, and leverage technology. The establishment of specialised police stations equipped to handle gender-based cybercrime cases is advocated, emphasising a multidisciplinary approach for policy formulation. Proactive measures informed by interdisciplinary collaboration, technological advancements, and policy reforms are deemed essential for creating a safer and more inclusive cyberspace in South Africa.

Table of Contents

DECLARATION REGARDING ORIGINALITY 2

ACKNOWLEDGEMENTS 3

ABSTRACT 4

CHAPTER ONE: INTRODUCTION 7

I. INTRODUCTION 7

II. BACKGROUND AND RATIONALE 7

III. LITERATURE REVIEW 20

IV. RESEARCH QUESTIONS 23

V. RESEARCH METHODOLOGY 23

VI. STRUCTURE OF DISSERTATION 24

CHAPTER TWO: ANALYSIS OF EXISTING LEGAL FRAMEWORKS 25

I. INTRODUCTION 25

II. UN MANDATES 26

III. INTERNATIONAL CONVENTIONS 28

IV. REGIONAL CONVENTIONS 31

V. LEGAL FRAMEWORKS IN SOUTH AFRICA 35

VI. CONCLUSION 51

CHAPTER THREE: THE SALIENT PROVISIONS OF THE CYBERCRIMES ACT 53

I. INTRODUCTION 53

II. ANALYSIS OF RELEVANT PROVISIONS PERTAINING TO GBV FORMS OF CYBERCRIMES 54

III. ABILITY OF CYBER CRIMES ACT TO GIVE EFFECT TO NSP ON GBV 91

IV. THE IMPLEMENTATION, REPORTING, AND ENFORCEABILITYCHALLENGES FACED WITHIN CYBERCRIME AND GBV 94

V. CONCLUSION 101

CHAPTER FOUR: RECOMMENDATIONS AND CONCLUSIONS ON HOW TO COMBAT GBV CYBERCRIMES 103

I. INTRODUCTION 103

II. SUMMARY OF FINDINGS 103

III. RECOMMENDATIONS 105

IV. CONCLUSION 118

BIBLIOGRAPHY 120

Articles 120

Case Law 125

Commissions of inquiry and government committees 126

Corporate bodies as authors – companies ,organisations , institutions *126*
Thesis *127*
Website Documents *127*
Legislation *129*

I. INTRODUCTION

This study aims to critically examine the reporting and enforceability challenges faced within the context of South African law concerning cybercrime forms of gender-based violence (GBV). It investigates the efficacy of current South African cyber law legislation in tackling cybercrime forms of GBV and South Africa's compliance with international treaties and jurisdictional issues.

II. BACKGROUND AND RATIONALE

Imagining gender-based cyber violence thirty years ago was inconceivable, as means such as open access to the internet and social media did not exist to commit online violence back then.[1] There is no uniform definition of gender-based cyber violence. However, the International Centre for Research on Women (ICRW) has defined it as "… an act perpetrated by individuals, aimed at causing harm to others due to their sexual or gender orientation, or by reinforcing detrimental gender stereotypes. This behaviour occurs through online platforms and mobile devices, encompassing activities such as stalking, cyberbullying, sexual misconduct, slander, discriminatory speech, and exploitation".[2] To tackle the onset of gender-based cyber violence, we need to first start by acknowledging that violence against women and girls, in traditional environments , is exceptionally high, has devastating consequences, and is deemed unlawful in international and Constitutional frameworks where it is recognised as a form of discrimination. However, only recently, the advancement of technology and related social media platforms has enabled the emergence of gender-based cyber violence.

During the 21st century, we have seen rapid growth and transformation in cyber technology. There are currently at least 5.35 billion people, with access to the internet.[3] Over 60 per cent of internet users lived in developed countries, and approximately 45 per cent were under 25. By 2017, it was estimated that mobile broadband subscriptions would have reached more than 70 per cent of the

[1] The Parliament Magazine. 2022. 'Gender-based cyberviolence: The new face of an old enemy''. Available at: <https://www.theparliamentmagazine.eu/news/article/genderbased-cyberviolence-the-new-face-of-an-old- enemy> [Accessed 18 April 2022].

[2] ICRW | PASSION. PROOF. POWER. 2022. Technology-Facilitated GBV: What is it, and How do we measure it? [online] Available at: <https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what- is-it-and-how-do-we-measure-it/> [Accessed 19 April 2022].

[3] L Pelchen and S Allen. 2024. Internet Usage Statistics in 2024. Available at https://www.forbes.com/home-improvement/internet/internet-statistics/

world's population[4] Internet connectivity has created limitless possibilities for billions of people worldwide and limitless capabilities for those involved in criminal activity. With this growth, new and advanced types of crime have emerged that are now committed through within the cyberspace domain.[5] Those wishing to engage in criminal activity have taken full advantage of the internet's power to commit various cybercrimes.[6]

GBV facilitated by technology, often termed technology-facilitated GBV (TGBV), has gained prominence in mainstream discourse since 2020 due to its escalating incidence. TGBV is a form of abuse by one or more people that causes harm to others based on their sexual or gender identity or enforces harmful gender norms in technological or online spaces. Furthermore, Bailey Poland noted this violence, stating the online harassment and abuse are intended to reinforce existing patterns of power and dominance over people who have a history of previously being oppressed. [7] Hence, it is essential to emphasize that although online abuse and harassment affect everyone, the experiences of women and Lesbian, Gay, Bisexual, Transgender, and Queer (LGBTQ+) individuals are influenced by gender dynamics. In a global context, TGBV is worryingly increasing. A recent survey by Amnesty International revealed that every 30 seconds, a woman receives a toxic degrading tweet, and 84 per cent of this total comprises black women. [8] In addition, women of colour are 34 per cent more likely to receive abusive remarks.

Additional studies involved a survey conducted by the IPU in 2016, which gathered responses from 55 female lawmakers across the globe. The findings revealed that 81.8 percent of these legislators experienced TGBV, encompassing frequent occurrences of degrading fake sexual images being circulated.[9] Another survey was conducted of women

[4] SM Mabunda "The South African legislative response to cybercrime" LLM dissertation. University of Western Cape (2021).

[5] DB Lucks *Cyberstalking: Identifying and examining electronic crime in cyberspace* (2004).

[6] A Stander, A Dunnet, J Rizzo J'A Survey of Computer Crime in South Africa' Venter et al… *Information Security South Africa* (2009).

[7] B Poland'Gendered Harassment, Abuse, and Violence Online' in O'Toole et al *Gender Violence, 3rd Edition: Interdisciplinary Perspectives* (2020).

[8] *Women abused on Twitter every 30 seconds - new study* (no date) *Amnesty International UK*. Available at: https://www.amnesty.org.uk/press-releases/women-abused-twitter-every-30-seconds-new-study (Accessed: 04 February 2024).

[9] *IPU study reveals widespread sexism, harassment and violence against…* Available at: https://www.ipu.org/news/press-releases/2016-10/ipu-study-reveals-widespread-sexism-harassment-and- violence-against-women-mps (Accessed: 04 February 2024).

parliamentarians from all over the world, and it was found that 41.8 per cent of the complainants had been extremely humiliated or there were sexually charged images of them which were circulated through social media, including photomontages showing them nude.[10]

a. Cybercrime

Cybercrime is an increasingly discussed subject across various platforms, including academic journals, computer magazines, news outlets, and online.[11] It has garnered widespread attention and notoriety in popular culture, social media, and general discourse.[12] At the same time, thistype of engagement has aided in raising awareness of the threats and challenges of cybercrime. The problem is exacerbated by the absence of a globally recognized definition of cybercrime. Cybercrime encompasses any unlawful actions that specifically target computers, computer systems, information networks, or data, as well as any illicit activities carried out directly through or with the assistance of these technological tools.[13] The United Nations (UN) provides two definitions of cybercrime. Cybercrime is defined narrowly as 'illegal behaviour directed through electronic operations that target the security of computer systems and the data they process.'[14] Moreover, cybercrimes can be defined as'any illegal behaviour committed using or in relation to a computer system or network, including illegal possession and offering or distributing information using a computer system.'[15]

The different forms of cybercrime can be defined under specific categories.[16] The first form ishybrid cybercrime, which is committed without the internet; however, cyberspace has createda platform for these forms of crime to escalate through this medium.[17] These cybercrimes include phishing, impersonation, and unlawful distribution of copyrighted materials, such as songs, films, and books. Phishing can be defined as the creation and use of different emails bycriminals to deceive people to gather financial, personal, and sensitive information such as credit card numbers or bank account information.[18] Impersonation can be

[10] L Hinson et al: 'Technology-facilitated GBV: What is it, and how do we measure it?' available at www.svri.org/sites/default/files/attachments/2018-07-24/ICRW_TFGBVMarketing_Brief_v8-Web.pdf .
[11] SM Mabunda "The South African legislative response to cybercrime" LLM dissertation. University of Western Cape (2021).
[12] Ibid.
[13] Ibid.
[14] United Nations. 2000.Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders' , available at http://bit.ly/2kjJFXN (accessed on 26 May 2022).
[15] Ibid
[16] J Muncie, D Talbot, and R Walters *Crime: Local and Global* (2010).
[17] Ibid.
[18] Binational Working Group (2006) . The word "phishing" is a variant of the word "phreaking", which was a term used in the early days of hacking, where a hacker would manipulate telephone systems to be able to make

defined as assuming the victim's identity to obtain more personal information regarding the victim.[19] The second form is traditional cybercrimes. These are crimes that would not exist without theinternet. Technology has allowed for the increase of the scope of criminal activity across borders and has ensured its effectiveness.[20] These include criminal behaviors with which our justice system is familiar. Such crimes include revenge pornography, cyber stalking, cyberbullying, harassment, and dissemination of malicious and hateful material. Revenge porn can be defined as non-consensual pornography involving the unauthorised uploading of photos or videos (typically of a sexual nature) of a person onto the internet as an act of vengeance, often committed by a former lover with the intention of humiliating and harassing the victim. Cyber stalking or bullying involves a series of actions that, while each may seem harmless onits own, collectively erode the victim's feeling of safety and provoke distress, fear, or alarm. They employ electronic devices for information exchange and communication, including email, instant messaging, text messages, blogs, mobile phones, social media platforms, instantmessages, and malicious websites, to engage in bullying or harassment, often through personal attacks or other methods.[21] Cyber-harassment and stalking can take the form of 'taunts, insults, and harassment over the Internet or text messages sent from mobile phones'.[22] This phenomenon has become pervasive among young people, with tragically results in some cases.[23] The most frequent forms of cyber harassment include threats of rape, sexually suggestive remarks, hate speech, which refers to insults directed at a person based on their identity (gender) and other traits such as sexual orientation, disability, or religion.

Revenge porn poses the greatest threat to women and children as it often deals with the malicious distribution of material to porn sites or any social network without the consent of the victim, intending to commit harm. Malicious distribution includes distributing the victim's intimate photographs and videos. The perpetrators may even send the information to the victims' employers or spouses to destroy the relationship or have the victim dismissed.[24] In

unauthorised long distance calls. 4.

[19] L Roberts 2008.'Cyber-Victimisation in Australia: Extent, Impact on Individuals and Responses' available at www.aic.gov.au/sites/default/files/2023-06/sr43_cybercrime_in_australia_2023.pdf

[20] J Muncie, D Talbot, and R Walters *Crime: Local and Global.* (2010)

[21] DS Wall, D 'The Internet as a Conduit for Criminal Activity'.in A Pattavina *information technology and the criminal justice system* (2005).

[22] Ibid.

[23] Ibid.

[24] T Goldsworthy, JCrowley, & M Raj, M (2015) 'Revenge porn is just one part of a changing picture of harassment' available at https://theconversation.com/revenge-porn-is-just-one-part-of-a-changing-picture-of-harassment-43703.

most cases, this is done by ex-partners who are bitter because the relationship has come to an end, and they want to shame and humiliate the victim in retaliation publicly. Furthermore, such a crime is not only perpetrated by an ex-partner; the motive is not always revenge. Images are often obtained by hacking into the victim's computer, social media, and cell phone, and the aim of doing this is to inflict real damage on the target's real-world life.

Furthermore, perpetrators can distribute images to obtain monetary benefits or boost social media status at the expense of another person. This has a negative impact on the victim as it may lead to suicide. There is also an increased number of websites dedicated to sharing revenge porn, where users can submit images alongside personal information such as the victim's address, employer, and links to online profiles. An additional related and devastating impact is that victims are now broadcasted live in the act of incidents of sexual assault and rape using social media as a to means an end.[25]

Harassment forms part of traditional cybercrimes. Harassment can be defined as spreading fear by constantly threatening and scaring the victim through constant voice messages or emails.[26] In this instance, the perpetrator may try to contact the victim repeatedly by using pornographic messages or messages of affection and discomfort to blackmail them into getting what they want.[27]

Lastly, the third form is true cybercrimes. This refers to crimes committed at the heart of cyberspace that only exist within the realm of the Internet. These include hacking and virtual reality theft that an individual purchases in real currency.[28] Hacking can be defined as unauthorised access to computer systems to acquire personal information, modify, or slander the victim.[29] Virtual reality is a new concept for law enforcement agencies around the world. However, millions of individuals connect in these 3-D worlds every day to socialise, shop, and attend online courses to learn.[30] Regrettably, lawbreakers have joined these virtual worlds, and all criminal activities are now present. Every day, ordinary "real world" crimes such as money laundering, theft of intellectual property, exchange of images of child abuse, and even

[25] Ibid.
[26] A Welsh & J A A Lavoie 'Risky eBusiness: An Examination of Risk-taking, Online Disclosiveness, and Cyberstalking Victimization' (2012) 6 (1) *Cyberpsychology: Journal of Psychosocial Research on Cyberspace.*
[27] Ibid.
[28] J Muncie, D Talbot, and R Walters *Crime: Local and Global.* (2010)
[29] SM Maat (2009) 'Cybercrime: a comparative law analysis' Available at https://uir.unisa.ac.za/bitstream/handle/10500/2056/03chapter3.pdf
[30] "Crime and Policing in Virtual Worlds"available at https://f3magazine.unicri.it/?p=360&format=pdf [Accessed 2 June 2022].

suspected terrorist activities occur in virtual worlds. For these reasons, new virtual worlds and communities present the criminal justice system with unique challenges. [31] Establishing rules for the virtual world and enforcing compliance with the law are critical problems experienced with virtual reality. Every conceivable crime and wrongdoing committed in the real world can also be perpetrated in the virtual world. There have already been reported instances of theft of virtual items that can be traded for virtual or actual currency and of sexual groping by one avatar[32] of another, causing genuine emotional harm to the player of the groped avatar.[33]

b. Efforts to combat cybercrime

Many international and regional organizations have made efforts to raise cybersecurity awareness. The Council of Europe (CoE), the Organisation for Economic Co-operation and Development (OECD), the (UN), the European Union (EU), and the International Criminal Police Organisation (Interpol) are some of the key participants in building international awareness and cooperation in this regard.[34] While there have been efforts within most international and regional organisations to promote cybersecurity awareness, there has been no indication of an African Union-led regional effort to combat cybercrime.[35] The only measure adopted thus far by the African Union (AU) to address cybercrime is the 2014 Convention on Cybersecurity and Personal Data Protection, which was adopted as part of Agenda 2063.[36] Despite the adoption of the convention by the AU, there appear to have been limited interventions undertaken to ensure its implementation or enforcement. Senegal has gone one step further than South Africa in ratifying the Convention, which became effective on 1 April 2017 in Senegal. In addition to the AU Convention, South Africa has introduced its legislation to combat cybercrimes. SouthAfrica's Cybercrimes Act[37] is a significant measure to address cyber-related offences. The effectiveness of mechanisms to combat cybercrime, such as legal frameworks, is highly dependent on the regional harmonization of domestic laws. Domestic legislation is insufficient on its own. Cross-country cooperation is necessary to combat a problem with no

[31] Ibid.
[32] Hdi.global. 2022. How virtual reality can create real-world legal trouble. [online] Available at: <https://www.hdi.global/en-za/infocenter/insights/2020/virtual-reality/> [Accessed 2 June 2022].
[33] An avatar typically refers to a digital representation of a person, often used in online forums, virtual worlds, or social media platforms. It can be a graphical image, a 3D model, or even just a username used to represent an individual.
[34] MD Goodman & SW Brenner 'The Emerging Consensus on Criminal Conduct in Cyberspace. (2002) 10(2) *International Journal of Law and Information Technology* 139-223.
[35] Y Turianskyi 'Balancing Cyber Security and Internet Freedom in Africa', (2018) Occasional Paper no. 275. *South African Institute for International Affairs*.
[36] Ibid.
[37] Cybercrimes Act 19 of 2020.

borders, suchas cybercrime. This harmonization does not exist in Africa in normative and policy frameworks.[38]

Despite its increased vulnerability to cybercrime, Africa continues to be a minor player in international and regional efforts to combat cybercrime. There is a palpable apathy among African leaders towards critical engagement with cybercrime, possibly due to a belief that thethreat is not as accurate as it appears in the West.[39] South Africa is an attractive target for cyberattacks for various reasons, including a dearth of cybersecurity investment, law enforcement training, and public awareness about cyberattacks.[40]

South Africa saw a 22% increase in cyber attacks in 2023.[41] A report compiled by the Norton Cybersecurity Insights in 2016 stated that 8.8 million South Africans were victims of cybercrime, which amounted to a loss of around R5.7 billion.[42] Cybercrime statistics recently posted by the South African Banking Risk Information Centre report that South African citizens lose more than R2.2 billion annually due to internet fraud and phishing attacks.[43]

c. Understanding GBV: Forms, Impact, and Legal Responses

Before delving into discussions surrounding gender-based cyber violence, it's crucial to first understand GBV. GBV refers to any violence targeted at an individual based on their gender or disproportionately affecting individuals of a certain gender. This encompasses actions causing physical, sexual, or psychological harm, as well as threats, coercion, and other forms of deprivation of freedom. Such violence arises from power imbalances rooted in gender differences among males and females.[44] GBV is complex as it manifests in many forms,

[38] United Nations Conference on Trade and Development (UNCTAD) (2013) 'Harmonizing Cyberlaws and regulations: The experience of the East African Community.'
[39] Y Turianskyi 'Balancing Cyber Security and Internet Freedom in Africa', (2018) Occasional Paper no. 275. *South African Institute for International Affairs*.
[40] W Mcanyana et al (2020) "Insight into the cyberthreat landscape in South Africa" available at https://www.accenture.com/za-en/insights/security/cyberthreat-south-africa
[41] SEACOM (2024) What cyber threats are likely to entail in 2024 available at https://seacom.co.za/news/what-cyber-threats-are-likely-to-entail-in-2024
[42] Van Zyl '8.8 million South Africans hit by cybercrime - study' 2016, available at, http://www.fin24.com/Tech/News/88-million-south-africans-hit-by-cyber-crime-study-20160707 (accessed on 18 April 2022.)
[43] Pay U 'SA companies under cyber-attack?' 2015, available at, https://www.payu.co.za/pressroom/ sa-companies-under-cyberattack (accessed on 18 April 2022).
[44] C Watts,& C Zimmerman 'Violence against women: global scope and magnitude.' (2002) 359 (9313) *The Lancet*1232-1237.

including physical, sexual and psychosocial abuse.[45] GBV encompasses a range of actions beyond just physical or psychological harm, such as humiliation, mental or sexual suffering, threats of harm, coercion, and various forms of restricting freedom, including cybercrimes based on gender.[46]

Domestic violence is the most prevalent type of GBV between intimate partners. This includes actual or threatened physical violence. In addition to sexual assault, coercion, and sexual harassment, domestic violence may also include sexual harassment.[47] Physical violence includes kicking, slapping, hitting, pushing, and the use of weapons.[48] Emotional violence includes acts of name-calling, disrespect, humiliation, and embarrassment.[49] These actions influence one's self-esteem and confidence.

Economic violence includes controlling a partner's economic freedom through control of their assets, access to money, and economic resources. This also includes hesitancy from a male partner for his female spouse or partner to work.[50]

Sexual violence can be described as any attempt to coerce a person into a sexual act or any action aimed at their sexuality, regardless of the perpetrator's relationship to the victim or the setting. This encompasses intimate partner violence, sexual assault, forced prostitution, exploitation, human trafficking, bondage, infanticide, and neglect.[51]

Lastly, femicide, which is the murder of a female partner by a male partner, represents the deadliest and most accurate form of GBV.[52] Intimate partner violence refers to behaviours occurring within an intimate relationship that result in physical, psychological, or sexual harm to one or both partners involved.[53] Coercion plays a pivotal role in sexual violence, covering a broad range of aggressive tactics. Beyond physical force, coercion can involve psychological manipulation, blackmail, or various threats, including the fear of physical harm, loss of employment, or failure to secure desired opportunities.[54]

---

[45] To ensure the provision of adequate and effective protection to all victims of sexual offences, and in particular to vulnerable groups such as women, children, and individuals with mental disabilities.
[46] Saferspaces.org.za. 2022. [online] Available at: <https://www.saferspaces.org.za/uploads/files/Soul_City_Literature_Review_GBV.pdf> [Accessed 25 May 2022].
[47] Tshwaranang Legal Centre (2012) 'Strengthening South Africa's Response to GBV through Prevention.'
[48] Ibid.
[49] Ibid.
[50] H Ludsin & L Vetten *Spiral of Entrapment: Abused Women in Conflict with the Law* (2005).
[51] Domestic Violence Act 116 of 1988.
[52] S Mathews(2010) 'Understanding Intimate Femicide in South Africa' (PhD diss., University of the Witwatersrand, Johannesburg)
[53] EG Krug et al… The world report on violence and health. (2002) 360 (9339) *The Lancet*, 1083-1088.
[54] Romi Sigsworth (2009) 'Anyone Can Be A Rapist… ' An Overview of Sexual Violence in South Africa Centre for

The issue of GBV has been identified as a crisis and a gross violation of human rights.[55] Academic scholars believe it has reached levels of disaster, which calls for immediate action.South Africa is equipped with progressive laws such as the Criminal Law: Sexual Offenses and Related Matters Act,[56] which was created to ensure to ensure the provision of adequate and effective protection to all victims of sexual offences, and in particular to vulnerable groups such as women, children, and individuals with mental disabilities.[57] The Domestic Violence Act[58] primary objective is to offer the highest level of protection against domestic abuse. Thelaw imposes a duty on state institutions, in particular the police, to ensure that survivors of domestic violence can file for protection orders prohibiting abusers from accessing a shared residence or the survivor's home or place of employment.[59] Promotion of Equality and Prevention of Unfair Discrimination Act[60] comprehensively deals with issues of discrimination and addresses residual factors of the promotion of equality in the workplace.[61] However, precise execution of the legislation is lacking.

When looking at the Domestic Violence Act, one of the main challenges hindering its implementation is that it was not costed when developed.[62] Moreover, although there is recognition that addressing GBV necessitates a multi-disciplinary strategy, the Act does not mandate the Department of Social Development to provide care and support services, nor does it impose obligations on the Department of Health or the National Prosecution Authority.[63] A 2012 Tshwaranang Study, which aimed to assess the implementation of the Domestic Violence Act, found that numerous police officers had limited awareness of their responsibilities as outlined in the Act's provisions.[64] One of the primary challenges faced by The Criminal Law: Sexual Offenses and Related Matters Act is the insufficient understanding of its

the Study of Violence and Reconciliation.

[55] Bazagan-Hejazi, et al. 'Patterns of intimate Partner violence: a study of female victims in Malawi.' (2013) 5) (1) *Journal of injury and Violence Research* 2.

[56] Sexual Offenses and Related Matters Act No 32 of 2007.

[57] Saferspaces.org.za. 2022. [online] Available at: <https://www.saferspaces.org.za/uploads/files/Soul_City_Literature_Review_GBV.pdf> [Accessed 25 May 2022].

[58] Domestic Violence Act 116 of 1998.

[59] Saferspaces.org.za. 2022. [online] Available at: <https://www.saferspaces.org.za/uploads/files/Soul_City_Literature_Review_GBV.pdf> [Accessed 25 May 2022].

[60] Promotion of Equality and Prevention of Unfair Discrimination Act 4 of 2000.

[61] Saferspaces.org.za. 2022. [online] Available at: <https://www.saferspaces.org.za/uploads/files/Soul_City_Literature_Review_GBV.pdf> [Accessed 25 May 2022].

[62] L Vetten, (2014) Rape and other forms of sexual violence . (2014) Policy Brief 72 *South Africa Institute of Security Studies*

[63] Ibid.

[64] Ibid.

provisions among various stakeholders. Despite its progressive definition of rape, there exists a substantial gap between community perceptions of rape and the legal definition outlined in the law. Furthermore, there are instances where stakeholders, particularly within the police and medico-legal services, lack a complete understanding of the provisions of the law.[65] The absence of specialized personnel within the justice system to handle sexual offenses has been identified as another factor contributing to the implementation challenges of these laws. In regions lackingspecialized sexual offenses courts, prosecutors already burdened with handling various aspects of criminal law are more likely to allocate limited time to preparing rape cases, further exacerbating the issue.[66] To end the cycle of domestic violence, a "multi-sectoral approach" must be implemented, beginning with reviewing the Domestic Violence Act with full financial backing for implementation and the need for a national strategic plan to address GBV in a multifaceted manner at all levels. It is imperative to confront systemic factors fostering violence, unemployment, poverty, heightened alcohol consumption, and increasing social alienation within the societal context.[67]

Despite these legislative measures to address this broad range of instances of GBV, South Africa leads the way with high numbers of sexual abuse and rape incidents.[68] A 2012 study revealed alarming rates of GBV in South Africa. It found that 77% of women in Limpopo, 51% in Gauteng, 45% in Western Cape, and 36% in KwaZulu-Natal had experienced some form of GBV during their lifetimes. The primary perpetrators of this violence were identified as men.[69] For example, in Gauteng, 76 per cent of men admitted to actively being involved in perpetrating GBV.[70] This is a clear indication that legislative measures are failing victims of traditional forms of GBV. As mentioned earlier, the challenges underscore this study's significance, aiming to investigate whether the implementation challenges facing existing GBV preventionand response legislation are replicated or even intensified in cases of gender-based cybercrime.

d. Exploring the Intersection of GBV and Cybercrime: Understanding Gender-Based

[65] Saferspaces.org.za. 2022. [online] Available at: <https://www.saferspaces.org.za/uploads/files/Soul_City_Literature_Review_GBV.pdf> [Accessed 25 May 2022].
[66] Ibid.
[67] Ibid.
[68] D.N. Bryen and J. Bornman, eds. *Stop Violence Against People with Disabilities: An International Resource* (2014) 41.

[69] Gender Links (2012) Research: Gender Violence 'A Reality in South Africa' (Johannesburg: Gender Links)
[70] Ibid.

Cyber Violence

Having established a conceptual distinction between cybercrime and GBV, it is imperative to explore the interconnections between these terms within the scope of this study. Gender-based cyber violence is an action which is carried out using the internet and mobile technology. Like conventional cybercrime, GBV includes examples such as stalking, bullying, sexual harassment, defamation, hate speech, and exploitation with an online presence.[71] The nature of the crime takes place in technological spaces where manufactured borders no longer exist as a barrier for perpetrators. Victims from different continents and regions can be identified, highlighting the need for dynamic and immediate response. The Internet acts as the means that facilitates different forms of violence against girls and women, which include sexual trafficking and the sex trade. Social networking has made it easier for perpetrators to identify, monitor, and obtain personal information about potential targets. Social networking provides perpetrators with the gift of anonymity and the whole world as a free target to spread acts of harassment and violence.[72]

Factors that challenge women's advancement in cyberspace include personal email accounts and social media accounts being hacked and revenge porn, whereby the perpetrator distributes these images without consent.[73] Most of the victims are women, and the possible repercussions are severe. There has been a widespread increase in revenge porn videos which has become common in South Africa. Women are also at risk through potential location tagging used to stalk victims as well, and the increase of information available online increases the risk for victims. Women are often at risk of cyberbullying and cyber-stalking, with many perpetrators now targeting children for the distribution of child pornography and hate groups being created to marginalize women based on their gender. Insufficient understanding and skill from local authorities exacerbates the problem women face, whereby such crimes may be deemed a type of sexual violence that extends beyond the traditional definitions of sexual violence.[74]

---

[71] ICRW | PASSION. PROOF. POWER. 2022. Technology-Facilitated GBV: What is it, and How do we measure it? [online] Available at: <https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what- is-it-and-how-do-we-measure-it/> [Accessed 19 April 2022].

[72] Africa.unwomen.org. 2022. [online] Available at: <https://africa.unwomen.org/sites/default/files/Field%20Office%20Africa/Attachments/Publications/2020/Background%20Paper_creating%20safespaces%20for%20young%20women%20and%20girls%20in%20Africa-Web.pdf> [Accessed 19 April 2022].

[73] ISS Africa. 2022. Cyberspace: new frontiers for gender violence - ISS Africa. [online] Available at: <https://issafrica.org/iss-today/cyberspace-new-frontiers-for-gender-violence> [Accessed 20 April 2022].

[74] Africa.unwomen.org. 2022. [online] Available at: <https://africa.unwomen.org/sites/default/files/Field%20Office%20Africa/Attachments/Publications/2020/Background%20Paper_creating%20safespaces%20for%20young%20women%20and%20girls%20in%20Africa-Web.pdf> [Accessed 19 April 2022].

The Association for Progressive Communications Women's Networking Support Programme has identified various factors which drive violence against women in cyberspace[75] Firstly, anonymity is the instrument of destruction, as potential perpetrators can remain anonymous and commit these atrocities without entering the public sphere or anyone knowing who they are. In addition, automation, which refers to technology that reduces essential human effort, allows potential abusers to check their partner's phone, monitor their social networking, and log into personal accounts. Expert knowledge is not needed to make use of these features.[76]

Potential abusers can act remotely and post sexual harassment or harassment messages from anywhere in the world, making it extremely difficult for victims to identify and act against perpetrators. Today, anyone can post videos and pictures at little to no cost via email or social media, which can be replicated in seconds thousands of times irrespective of the type of content posted. Lastly, with cyber-space, tracking down and deleting a particular image or video circulation is almost impossible. This can, unfortunately, follow victims in school, work, and at home, leaving a long-lasting impact.[77]

"Take Back the Tech," which is a campaign created to regain communication technology from the hands of perpetrators to end violence against women and girls, has identified different categories of cyber technology violence, showing how technology aggravates traditional forms of GBV.[78] Online harassment and cyberstalking are the most common and most visible forms of technology-related violence against women. This category deals with harassing messages on social media, online comments of harassment and tracking the activities of women through social networking sites. Technology plays an active role in creating an environment of violence against women, for example, forwarding a sexist joke that women are less equal and valuable than men or starting a Facebook chat group to promote different ways to abuse women sexually.[79]

Many communities are targeted because of their gender, sexual orientation, and political

[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Ibid.
[79] Ibid.

views.[80] Women activists who believe and speak up about feminism are often ridiculed and receive threats online, while technology is used as an ally to recruit potential victims into violent situations.[81] For example, traffickers use chat rooms and websites to communicate fraudulent postings and advertisements, enticing victims to communicate personal information.[82]

Gender-based forms of cybercrime have long-lasting and devastating effects on the safety and security of women and girls, constituting a violation of multiple rights enshrined in South Africa's Constitution. This includes the right to freedom and security of the person, equality, and dignity, as outlined in Section 9 of the Constitution.[83] Consequences experienced include personal relationships being destroyed, loss of dignity, psychological distress, violation of one's right to privacy, public humiliation, loss of opportunity, damage to reputation, and financial losses.[84]

Many victims often struggle with adequate recourse due to the lack of legal and regulatory agencies to assist them. The medieval attitude still lives and breathes in a society where many men and women accept or condone violence against women and believe that women and girls are less valuable.[85] This includes society leaders such as politicians, service providers, police, justice officials, health workers, community leaders, and faith-based leaders.[86] Women around the world have had different experiences. As a result, it is impossible to generalize women's experiences into a single point of view that applies to all women. However, generalizations will have to be made when considering the threat of gender-based cyber violence.

This study aims to analyse the legal frameworks concerning gender-based cybercrime and critically assess the cybercrimes Act's effectiveness in addressing this particular form of cybercrime. These frameworks will be assessed to determine whether they affect South Africa's obligations in terms of international and Constitutional law and provide adequate recourse to victims of this form of crime. The study will further draw on international best practices in combating gender-based cybercrime to develop recommendations on how South Africa can address this form of GBV.

[80] Ibid
[81] Ibid
[82] Ibid
[83] Constitution of the Republic of South Africa, 1996.
[84] Ibid.
[85] Ibid.
[86] Ibid

III. LITERATURE REVIEW

As with any of the great technological inventions, the Internet can be used for the benefit of humanity or as a means of systemic loss and suffering. Over time, the internet has developed into a mechanism for creating a parallel universe in the form of the Dark Web.[87] The Dark Web refers to a hidden part of the internet accessible only through specific software, where users can anonymously engage in activities outside the scope of traditional search engines and web browsers. Inadvertently, the constant evolution of technologies, such as the Internet, spawns new types of computer-enabled crimes, targets, and perpetrators.[88] Newer and more specialized computer-crime laws are required to combat modern criminals and the unusual crimes they commit using the internet and computing technologies.[89]

On the African continent, cybercriminal activity is at its highest due to the limited understanding of information technologies, the ignorance and absolute trust in the safety of transacting on the internet, is primarily because of high illiteracy levels in many African countries.[90] There are few suitable laws to deal with cybercrimes in many of the countries in Africa.[91] As a continent primarily focused on combating the HIV/AIDS pandemic, poverty, rising unemployment, primary service delivery, crime, and eradicating corruption, developing cyber law receives secondary attention, leaving the continent vulnerable to the growth of cybercrime.[92]

There is extensive literature available on the issue of gender-based cybercrime in South Africa. The intersection between cybercrime and gender has not been extensively addressed globally. Prior research is relatively old and does not address the questions this study aims toaddress. Academics view the legislation governing information and communications technology use in South Africa as largely incoherent.[93]

---

[87] Ibid

[88] F Cassim 'Formulating specialised legislation to address the growing spectre of cybercrimes: a comparative study' (2009) 12 *Potchefstroom Electronic Law Journal* 37

[89] D Glance 'What is the Dark Web?' (2017) available at http://theconversation.com/explainer-what-is-thedark-web-46070, (accessed on 26 May 2022).

[90] International Telecommunication Union 'Global Cybersecurity Index 2017 Africa Report', 2017, available at http://bit.ly/2C3zrRn, accessed on 26 May 2022.

[91] Ibid.

[92] F Cassim 'Formulating specialised legislation to address the growing spectre of cybercrimes: a comparative study' (2009) 12 *Potchefstroom Electronic Law Journal* 39.

[93] U Pukwana & M Kyobe 'Investigating the Misalignment in the Existing ELegislation of South Africa' (2016)

Cassim observes that prior to the enactment of the Electronic Communications and Transactions Act 25 of 2002 (referred to as ECTA thereafter), existing common law and statutory principles were utilized to address online offenses. For instance, indecency laws could be applied to combat child pornography, fraud statutes could target cyber fraud, and crimen injuria laws could be employed in prosecuting cyber smearing. However, despite these measures, a legislative void remained, underscoring the need for a specialized framework explicitly addressing cybercrime, especially in cases of gender-based cyber offenses.[94]

Scholars Grobler and Dlamini have provided empirical evidence elucidating the magnitude of cybercrime in South Africa, affirming a pressing issue that demands prompt intervention.[95] Grobler and Dlamini describe how vulnerable South Africa is to cyber-attacks. The limited cybercrime literature accessible in South Africa is frequently generated by the scientific and technology industry or written from a business perspective.[96] Whatever the case may be, it is from these scholars that one may deduce that cybercrime is a legitimate problem. Unfortunately, there is a scarcity of legal literature that expressly addresses the link between cybercrime and GBV and how government might respond to gender-based cybercrime.

The Cybercrimes Act represents South Africa's response to formulate a legislative response to cybercrime. This Act follows the Electronic Communication and Transactions Act 25 of 2002, or ECTA, which was created to 'provide for the facilitation of electronic communication and transactions" and "to develop a national e-strategy for the country but lacked precise implementation of gender-based cybercrime.'[97] Mabunda concluded that the ECTA was a steppingstone in the fight against cybercrime, but its intended purpose was never to legislate on cybercrime in South Africa.[98] Cybercrime, specifically gender-based cybercrime, was never a concern of the academy in South Africa and only gained momentum with cybersecurity

CONF-IRM 2016 Proceedings. 38.

[98] F Cassim "Addressing the Challenge Posed by Cybercrime: A South African Perspective" 5(3) *Journal of International Commercial Law and Technology* 118-123.

[94] M Grobler and Z Dlamini 'Global cyber trends a South African reality.' IST-Africa 2012, Dar es Salaam, Tanzania, 9-11 May 2012

[95]M Grobler and Z Dlamini 'Global cyber trends a South African reality.' IST-Africa 2012, Dar es Salaam, Tanzania, 9-11 May 2012

[96] Long Title of ECTA.

[97]SM Mabunda "The South African legislative response to cybercrime" LLM dissertation. University of Western Cape (2021).

"

[98]Ibid."

professionals[99]. Hence, this study is important in examining the newly enacted Cybercrimes Act to fight gender-based cybercrime.

Cyberlaw scholars such as Cassim have noted that the ECTA was a significant step in materializing the fight against cybercrime but had room for improvement.[100] This view is supported by Snail, who applauded South Africa for taking the fight against cybercrime through the ECTA; even though it was deemed imperfect, it created legal certainty about what constitutes cybercrime and what does not.[101]

Cassim suggests that there is a need for specialized cyber tribunals or courts to help with cybercrime prosecution. She claims this must be combined with a balanced approach to fundamental human rights protection and the necessity for successful cybercrime prosecutions.[102] This is a viewpoint shared by Snail, who applauds South Africa for adopting legislative efforts under the ECTA to address emerging crimes, albeit he adds that these steps should be scrutinized. This is particularly relevant in addressing gender-based cybercrime which represents an imminent threat against women and children.[103]

Grobler, Van Vuuren, Zaaiman discuss how South Africa does not have a cyber defence strategy.[104] Moreover, research also argues that the constant rise and changing nature of cybercrime, which has not evolved into something as dangerous as gender-based cybercrime, requires that our government establish new mechanisms to address such issues related to cybercrime.[105]

This research builds upon the existing literature, addressing a notable gap in comprehensive critiques of gender-based cybercrime within the framework of the Cybercrimes Act. This study contributes to the scholarly discourse by providing such a critique.

---

[99] Ibid.

[100] F Cassim "Addressing the Challenge Posed by Cybercrime: A South African Perspective" 5(3) *Journal of International Commercial Law and Technology* 118-123

[101] S Snail "Cybercrime in South Africa – Hacking, Cracking and Other Unlawful Online Activities" (2009) 138 *Journal of Information, Law & Technology* 1-13.

[102] F Cassim "Addressing the Challenge Posed by Cybercrime: A South African Perspective" 5(3) *Journal of International Commercial Law and Technology* 118-123

[103]S Snail "Cybercrime in South Africa – Hacking, Cracking and Other Unlawful Online Activities" (2009) 138 *Journal of Information, Law & Technology* 1-13.

[104] M Grobler, J Van Vuuren, J Zaaiman, 'Preparing South Africa for Cybercrime and cyber defense' (2013) 11 (7) *Journal of Systemics Cybernetics and Informatics* 32-41.

[105] J van Vuuren, MGrobler,and J Zaaiman'The influence of cyber security levels of South African citizens on national security.' (2012) *7th International Conference on Information Warfare and Security*

The above studies have begun to provide insight into how there is a need for harmonization of legal and technical solutions to the problem of cybercrime. The international community, including governments and supranational organizations, has recognized that such harmonization is transnational and borderless. The Council of Europe (CoE), the Organization for Economic Co-operation and Development (OECD), the United Nations (UN), the European Union (EU), and the International Criminal Police Organization are among the critical partners in raising international awareness and cooperation in this area (Interpol). They have set the tone for how states should respond to cybercrime as the primary drivers of awareness.[106]

IV. RESEARCH QUESTIONS

The following questions form the foundation for the proposed study:

1. Does the current legislative framework governing cybercrime forms of GBV in South Africa adequately address gender-based cyber violence. What are the implementation and enforcement challenges?
2. Does this framework give adequate effect to South Africa's obligations under international law provisions?
3. What are the implications for strengthening South Africa's response to cybercrime and GBV?

V. RESEARCH METHODOLOGY

This dissertation is a non-empirical study based on desktop research of relevant primary and secondary sources. The study is based on qualitative research. The qualitative investigation is founded on extensive desk research of primary and secondary sources. National and international agreements, statutes, legislation, case law, databases, textbooks, journal articles, cyberspace sources, magazine articles, newspaper articles, interviews, presentations, news reports, and expert opinions are all sources.

[106] SM Mabunda "The South African legislative response to cybercrime" LLM dissertation. University of Western Cape (2021).

VI. STRUCTURE OF DISSERTATION

The structure for this study is as follows:

Chapter 1 is the introduction of the dissertation. It establishes the topic, and it consists of an overview of what cyber-crime is and the relevance to violence against women. Additionally, it provides context for the study by outlining its rationale, objectives, and significance. Additionally, this chapter contains the literature review of the primary and secondary sources of work consulted during the writing of this dissertation followed by the research questions that will be evaluated,

Chapter 2 provides an overview of the international conventions and treaties addressing states' obligations in terms of international law to eradicate, report, and respond to gender-based cyber violence. The study investigates South Africa's legislative framework concerning gender-based cybercrime was undertaken, with a specific focus on the Electronic Communications and Transactions Act (ECTA) and its limitations in addressing this issue. Following this, the study presents a comprehensive critical analysis, encompassing the Cybercrime Act, its regulations, and enforcement mechanisms, to assess its efficacy in addressing gender-based cyber violence. This analysis establishes a fundamental groundwork for the central context of this dissertation.

Chapter 3 delves into a comprehensive examination of the Cybercrime Act in South Africa, meticulously dissecting its provisions, implications, and enforcement mechanisms.

Chapter 4 deals with the implications of strengthening South Africa's response to gender-based cyber violence by providing recommendations and conclusions. This final chapter comprises conclusions, a summation of the issues discussed, and recommendations and changes needed to combat gender-based cyber violence.

CHAPTER TWO: ANALYSIS OF EXISTING LEGAL FRAMEWORKS

I. INTRODUCTION

Over the past two decades, internet and social media penetration levels in Africa have witnessed a significant increase. In 2010, William Lynn, America's Deputy Secretary of Defense, emphasized the growing importance of Cyberspace, referring to it as a "man-made domain." He highlighted that Cyberspace had become "just as critical to military operations as land, sea, air, and space."[107] Cyberspace has opened up a connected world for approximately three billion individuals who are now linked to the internet. This number is rapidly expanding, and projections indicate that by 2020, it is anticipated to reach five billion people, utilizing an estimated 50 billion gadgets.[108] Regarding functionality, Africa's internet usage in March 2017 was 9.3 per cent, whereas the rest of the world's usage was 90.3 per cent.[109] As of March 2017, 27.7 percent (0.345 billion) of Africa's overall population of 1.25 billion (which represents 16.6 percent of the global population) were internet users, with 0.146 billion possessing Facebook pages.

By June 30, 2017, the number of internet users in Africa was estimated to be 0.388 billion, constituting 31.2 percent of the total world internet users and representing 10.0 percent of the total world internet users. In contrast, the rest of the world had an internet penetration rate of 55.8 percent, surpassing the global average of 51.7 percent. When compared to the global context, Africa's susceptibility to cyberattacks becomes apparent. Globally, 54 percent (3.39 billion) of the 6.27 billion people are internet users, contributing to 90.7 percent of global participation, with 1.53 billion Facebook members.[110]

The widened increase in internet activity opens billions of people to unknown avenues of gender-based forms of cybercrimes, which places importance on proper cyber security awareness and formalized training for this domain. The United Nations (UN) has underlined that the continent

[107] R Thomas *CyberWar will not take Place* (2013).
[108] Ibid
[109] Ibid
[110] The 2017 population estimates are based mainly on figures from the United Nations Population Division and local sources. The internet usage numbers come mainly from data published by WWW, ITU, the Nielsen Company, Facebook, and other trustworthy sources. Data from this table may be cited giving the due credit and establishing an active link back to Internet World Stats

benefits significantly from the growing internet penetration as increased internet usage would empower regular people to gain skills or be utilized for online learning, service delivery, and political participation.

However, aside from the initial optimism, there is enough evidence to suggest that the internet and its ancillary digital media technologies can expose citizens to many forms of harmful and hurtful speech. Online comments, which may be classified as hate speech, have risen in prominence in the digital era. Hate speech is defined as any expression, gesture, or behaviour that offends, threatens, or insults individuals or groups based on characteristics such as race, ethnicity, religion, sexual orientation, gender, or any other. While freedom of expression is a fundamental right according to our Constitution, it does not include hate speech that promotes sexual harassment online, discrimination, animosity, or violence, which, therefore, results in the creation of new and evolved cybercrimes.[111] As technology evolves, new cybercrimes will emerge, requiring new cyber laws to be introduced to respond to these rapid changes or to bring about redress.

This chapter will begin with an overview of key international agencies established to address GBV and their efforts to eradicate, report, and respond to gender-based forms of cybercrime as outlined in various conventions and treaties. Following this, it will examine relevant Constitutional provisions and South Africa's legislative framework, elucidating the state's obligations in combating gender-based cybercrime.

II. UN MANDATES

a. The United Nations Special Rapporteur on Violence Against Women, its Causes and Consequences (the UN Special Rapporteur)

In 1994, the UN established the role of Special Rapporteur on violence against women, with a mandate to gather information on violence against women, recommend measures at various levels to eliminate such violence, and address its causes and consequences.[112] This work involves country visits, annual and thematic reports, and consultations with diverse entities. The recognition of the digital dimension of gender-based violence (GBV) dates back to 2006,marking

[111] *What is hate speech? United Nations.*

[112] Human Rights Council, 1994.

the beginning of a necessary inquiry into the utilization of Information and Communication Technologies (ICTs) to identify and confront emerging manifestations of violence.[113] The Human Rights Council emphasized the protection of offline rights online.[114] In 2018, a groundbreaking report was issued by the UN Special Rapporteur, centering on online violence and violence facilitated by Information and Communication Technologies (ICTs) against women and girls. This report introduced a comprehensive framework for examining the impact of emerging technologies on preventing violence, safeguarding individuals, prosecuting perpetrators, and offering avenues for recourse.[115] The report is a foundation for subsequent UN activities, country reports, and regional work in this field.

The UN Special Rapporteur adopts the term "ICT-facilitated violence against women" as the most inclusive, using "online violence against women" for user-friendly communication. The definition encompasses any GBV involving ICT, such as mobile phones, the Internet, social media, or email, disproportionately affecting women. Recognizing the rapid development of digital technology, the UN Special Rapporteur refrains from attempting to define and catalogue all forms of online violence against women. The digital dimension of violence against womenis included in country visit reports, acknowledging efforts to address online violence in various countries. Thematic reports emphasize the significance of online and technology-facilitated violence against women, highlighting its impact on women journalists and media participation.[116] However, the intersection of violence against women and cybercrime, including various forms of GBV online, remains a growing global concern. Cyber-related GBV manifests in online harassment, stalking, non-consensual sharing of intimate images, and other digital abuses.

> The UN Special Rapporteur on violence against women, its causes and consequences, as well as the UN Special Rapporteur on the right to peaceful assembly and association, have issued recommendations to combat online GBV. These include, for states, enacting new laws to prohibit emerging forms of online GBV and, for Internet intermediaries, greater transparency in decision-making and applying online GBV standards. Participation of WHRDs, women's organizations, and other civil society actors in implementing these recommendations, as well as increasing public awareness and resilience in the face of online attacks on women and girls, will be critical.

[113] UN General Assembly, 2006.

[114] Human Rights Council, 2016.

[115] All reports on the country visits of the UN Special Rapporteur on violence against women and girls, its causes and consequences are available at: www.ohchr.org/en/special-procedures/sr-violence-against- women/country-visits

[116] Human Rights Council, 2020.

a. The United Nations Entity for Gender Equality and the Empowerment of Women (UN Women)

The United Nations Entity for Gender Equality and the Empowerment of Women (UN Women) has emphasised eliminating gender-based forms of cybercrime. The burning issue is that online spaces and technologies have become tools for the continued systemic oppression of women and girls. Addressing gender-based forms of cybercrime is imperative for upholding humanrights and promoting equality. It is commendable that UN Women has prioritized this issue, especially given its prevalence in regions like Africa. By recognizing cyber violence as a violation of fundamental rights outlined in various legal frameworks, including national Constitutions and international agreements, efforts can be directed towards developing comprehensive strategies for prevention and intervention. It is crucial to raise awareness, strengthen legal protections, and provide support services for victims, while also addressing the underlying societal attitudes and inequalities that perpetuate such crimes.[117]

III. INTERNATIONAL CONVENTIONS

a. Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW)

The UN Committee on the Elimination of Discrimination against Women (CEDAW) was founded in 1982 with the purpose of supervising the implementation of the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW Convention). [118] The CEDAW Committee consists of twenty-three independent experts tasked with reviewing the national implementation of the CEDAW Convention. They assess progress through issuing 'concluding observations'. Furthermore, CEDAW addresses individual communications alleging violations of women's rights and can also launch inquiries into severe or systematic violations.[119] The committee also formulates General Recommendations, offering authoritative statements on the legal duties assumed by state parties and guiding the interpretation of treaty

[117] Ibid
[118] UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, United Nations, Treaty Series, vol. 1249, p. 13, 18 December 1979n
[119] UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, United Nations, Treaty Series, vol. 1249, p. 13, 18 December 1979

provisions.

In 1992, CEDAW adopted General Recommendation No. 19 on violence against women, subsequently updated in 2017 as General Recommendation No. 35 on GBV against women.[132] CEDAW defines discrimination against women as "any distinction, exclusion, or restriction based on sex," emphasizing that GBV falls within the Convention's scope.[120] It characterizes GBV as violence directed at women because of their gender, constituting a violation of their human rights.

CEDAW emphasizes the significance of adopting an intersectional approach to understanding GBV, recognizing the diverse characteristics and identities that impact individuals' experiences of violence and discrimination. Particularly noteworthy is General Recommendation No. 35, which explicitly acknowledges online and technology-facilitated violence as a novel form of GBV falling within CEDAW's purview.[121] The committee integrates the digital dimension into various General Recommendations, such as No. 33 (2015) on women's access to justice and No. 36 (2017) addressing the impact of cyberbullying on girls.[122] Recent country reports, including those for Morocco, Ecuador, Sweden, and Denmark, applaud legal reforms targeting online and technology-facilitated violence.[123]

CEDAW, established as a milestone for advancing women's rights, is often termed the international Bill of Rights for women. It has defined discrimination against women, set a comprehensive agenda for national action, and urged states to commit to measures ensuring gender equality. Article 16 emphasizes women's right to choose a spouse, safeguarding them from early marriages freely.[124] Article 8 mandates states to provide equal opportunities for women to represent governments internationally and participate in international organizations.[125]

CEDAW's 25 General Recommendations guide state parties in elaborating on their views and obligations under the Convention.[126] The reporting mechanism allows countries to submit reports every four years, presenting a transparent overview of achievements, challenges, and commitments regarding women's advancement. While CEDAW may not explicitly mention

[120] UN Women CEDAW General Recommendation.
[121] Council of Europe, 2022. *The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform* Online: OHCHR.
[122] UN Women 'CEDAW General Recommendation.
[123] UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, United Nations, Treaty Series, vol. 1249, p. 13, 18 December 1979]

[124] Ibid.
[125] Article 8 of CEDAW.

[126] UN Women 'CEDAW General Recommendation.

cybercrime, its holistic approach to GBV encompasses various mediums through which violence occurs. The Convention emphasizes the imperative to safeguard women from violence and harmful practices, regardless of the platform. In the realm of cybercrime and GBV, nations acknowledge the intersection of technology and violence against women. Legal frameworks are adapting to address cyber-harassment, online stalking, and digital abuse as extensions of GBV. CEDAW serves as a cornerstone for advocating policies and legal measures to combat GBV, including its manifestations in cyberspace. It encourages member states to enact laws protecting women from online forms of violence and harassment.[127]

a. Beijing Declaration and Platform for Action (BPA)

In 1995, during the Fourth World Conference on Women, the Beijing Platform for Action urged states, media institutions, associations, and Non-Governmental Organizations (NGOs) to increase the participation and access of women to roles in media and emerging communication technologies, emphasizing the importance of their involvement in decision-making processes.[128] It is unfortunate that research indicates women in public roles, including journalists, politicians, and human rights activists, are among the most targeted groups for gender-based cyber violence.[129] This phenomenon is exacerbated, particularly for targeted women belonging to minority groups, especially in environments where political opinions are expressed, such as during election campaigns or while holding political office.[130]

The BPA is acknowledged as the world's pioneering, extensive, and transformative development agenda.[131] Women from across the globe gathered in Beijing to witness this transformative moment for women globally.

Governments and civil societies were encouraged to work together to guarantee the fulfillment of women's and children's rights, implementing all required measures to eliminate any form of discrimination against women and girls.[132] In the past twenty-two years, the Beijing Platform for Action (BPA) has played a crucial role in driving substantial transformations in the lives of women. Its focus on promoting equality, development, and peace has contributed to the

[127] Council of Europe, 2022. *The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform* Online: OHCHR.
[128] Beijing Declaration and Platform for Action of 1995.
[129]. Chanana, P., 2017. *The Role of UN Women Towards the Development and Advancement of Women in Southern Africa: A Critical Comparison between South Africa and Zimbabwe* (Master's thesis, University of Pretoria (South Africa)).
[130] Ibid.
[131] "We need a global movement of solidarity for gender equality"- available at http://www.unwomen.org/en/news/stories/2014/11/ded-speech-from-africa-regional-b20-review.

[132] Ibid.

advancement of humanity as a whole.[133] Efforts are directed towards ensuring that all women and girls, regardless of the obstacles they encounter, enjoy equal access to all rights and fundamental freedoms. The declaration underscores the importance of supporting the development of women and girls of all ages to their maximum potential, ensuring their equitable participation in constructing a better world and enhancing their contribution to the development process.

The Declaration acknowledges poverty as a challenge experienced by women, which includes issues such as early marriages, limited access to education, social and political discrimination, and exclusion. Governments were urged to eradicate disparities between women and men in accessing education and achieving educational outcomes across all levels and forms of education.

IV. REGIONAL CONVENTIONS

In order to facilitate the harmonized implementation of diverse instruments promoting gender equality and equity, which SADC Member States have ratified across regional, continental, and international levels, this section explores regional conventions. These instruments encompass various significant agreements. Among them are the SADC Declaration on Gender and Development (1997) and its Addendum (1998). They include the Millennium Development Goals (2000), the African Charter on Human and Peoples' Rights, the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (2003), and any other pertinent legal frameworks.[134]

a. African Union Convention on Cyber Security and the Protection of Personal Data

In the effort to address Gender-Based Forms of Cybercrimes, the imperative lies in the harmonization of legal frameworks across Africa. This harmonization is crucial for combating cybercrime and fostering international cooperation in effectively addressing this multifaceted challenge. In 2014, the African Union adopted the African Union Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention.[135] This convention aims to standardize the laws of African nations concerning electronic commerce, data protection, governance of cybersecurity, and the control of cybercrime.[136] In addition to

[133] Beijing Declaration and Platform for Action of 1995.

[134] SADC Protocol on Gender and Development (2016).

[135] AU General Assembly (2014) African Union Convention on Cyber Security and Personal Data Protection

[136] See Preamble, AU Convention on Cybersecurity and Personal Data Protection, 2014.

defining the goals for the information society in Africa, the Convention endeavours to strengthen the current ICT laws in member states and Regional Economic Communities.[137]

As a result, the Convention employs "technology-neutral" language to establish both substantive and procedural criminal law provisions intended to govern cybersecurity andcombat cybercrime within AU Member States. Apart from delineating these provisions, the Convention imposes considerable responsibilities on member states to develop national cybersecurity policies and create legal, regulatory, and institutional frameworks conducive to effective cybersecurity governance and the regulation of cybercrime.[138] This approach appearsto exceed that of the Council of Europe Convention on Cybercrime,[139] which requires Member States to criminalise cybercrimes by establishing substantive criminal law measures and procedural and international law enforcement cooperation mechanisms.

Article 24:2 of the Convention requires Member States to initially adopt "appropriate and adequate" strategies when executing their national cybersecurity policy. This encompasses measures such as legal reform and development, capacity building, fostering public and private partnerships, and raising awareness about cybersecurity. Importantly, the Convention recognizes each Member State's sovereign right to adopt any strategy it deems suitable or appropriate for implementing its national cybersecuritypolicy.[140]

Article 25 (1) mandates Member States to criminalize various forms of cybercrime as part of the effort to combat Gender-Based Cybercrime. These offences encompass a range of activities, including but not limited to child pornography,[141] unauthorized interception of computer data, unauthorized access to computer systems,[142] computer data forgery,[143] and preparatory offences linked to the misuse of computing devices. These preparatory offences involve unlawful production, importation, possession, or dissemination of computer

equipment, programmes, or any other device or data specifically designed or adapted for

[137] Ibid.
[138] The technology neutrality principle proposes that “legislation should define the regulation to be achieved and should neither impose, nor discriminate in favour of the use of a particular type of technology to achieve those objectives”. See European Commission (1999) Towards a New Framework for Electronic Communications Infrastructure and Associated Services. Brussels: European Commission, p. 539. See generally, Sharpe A. (2009) Communications Technologies, Services and Markets. In: Ian Walden (ed.) Telecommunications Law and Regulation. 3rd ed. New York: Oxford University Press, p. 53
[139] The Council of Europe Convention on Cybercrime, 23 November 2001.
[140] UJ Orji, ‘Examining Missing Governance Mechanisms in the African Union’ (2014).
[141] See Article 24:2 AU Convention on Cybersecurity and Personal Data Protection.
[142] See Article 29:3(1)
[143] See Article 29:2(b)

committing cybercrime offences.

Article 25(1) of the Convention stipulates that member states must establish effective procedural mechanisms for prosecuting cybercrime offenses. These mechanisms typically involve facilitating the search, seizure, or preservation of digital evidence, as well as the interception of electronic communications. This strengthens the legal capabilities of law enforcement authorities to investigate and prosecute cybercrime offenses. Member States are encouraged to harmonize their substantive and procedural legal measures with international best practices in combating cybercrime. Additionally, Article 25(2) of the Convention mandates Member States to create structures or institutions necessary for cybersecurity governance. Similarly, Article 27(1) requires Member States to adopt measures to establish an appropriate institutional mechanism responsible for cybersecurity governance. This responsibility entails establishing national institutions dedicated to combating cybercrime, responding to cybersecurity incidents, and facilitating international cooperation in managing such incidents.[144]

Article 26 of the Convention delineates Member State obligations to foster a cybersecurity culture among all stakeholders, encompassing government institutions, enterprises, and civil society. Member States are mandated to cultivate a cybersecurity culture within their national territories by promoting awareness among the public and delivering cybersecurity education and training.[145]

Through the promotion of certification courses for ICT professionals in the private and public sectors.[146] Member States must develop a public-private partnership model that enlists the participation of industry organisations, civil society, and academia in promoting a culture of awareness for cybercrimes.[147]

Within the African Union, the Convention, as outlined in Article 28(4), establishes a framework that encourages international cooperation on cybersecurity and cybercrime control. This involves leveraging existing channels for international cooperation to address cyber threats, enhance cybersecurity, and foster dialogue among stakeholders.[148]

~~The Malabo~~The Malabo Convention was ratified by the requisite 15 Member States and came into effect on 8 June 2023. Presently, only 13 Member States have ratified the

[144] See Article 29:2(b).
[145] See Article 27:2 AU Convention on Cybersecurity and Personal Data Protection.
[146] See Article 26:2 AU Convention on Cybersecurity and Personal Data Protection.
[147] See Article 26:4 AU Convention on Cybersecurity and Personal Data Protection
[148] See Article 26:3 AU Convention on Cybersecurity and Personal Data Protection

Convention, with South Africa being an exception. The Malabo Convention explicitly emphasizes the need for legislation and harmonization against cybercrime, stressing that legislative measures adopted should align with international best practices. This approach aims to facilitate regional harmonization of legal measures related to cybercrime.

The articles contained in the convention are a step in the right direction to combat the issue of Gender Based forms of Cybercrime as it recognizes this form of violence and provides us with tools needed to combat such an issue.

a. The Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (Maputo Protocol)

The Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa, commonly referred to as the Maputo Protocol, is an international human rights instrument created by the African Union. Initially endorsed by the "Assembly of the African Union" on July 11, 2003, in Maputo, Mozambique, the Maputo Protocol seeks to guarantee that all women in Africa are granted protection against discrimination, inclusion in matters of gender, and the safeguarding of human dignity.

Articles 2, 3, and 4 of the Maputo Protocol explicitly advocate for the eradication of all formsof discrimination against women, regardless of their sexual orientation or gender identity.[149] The Protocol pledges to bolster local, national, regional, and continental efforts aimed at eliminating discrimination against women. Furthermore, it recognizes the rights of women and girls to life, integrity, security, and dignity. In 2015, the African Union introduced the Revised Maputo Plan of Action, which broadens its scope to include African marginalized groups.[150] The principal aim of the Revised Plan is to advance the attainment of the sexual and reproductive health and rights (SRHR) targets delineated in the Sustainable Development Goals (SDGs), underscoring the critical role of the Maputo Protocol in championing inclusion in Africa.[151]

Article 2 deals explicitly with eliminating discrimination against women, whereby it calls on the state to undertake institutional and legislative measures to eradicate all forms of discrimination against women. In addition, the state has a duty through public education and communication strategies within society to eliminate discrimination between sexes and harmful cultural practices.[152] Article 4 explicitly addresses the right to integrity, life, and

[149] See Article 28:4 AU Convention on Cybersecurity and Personal Data Protection
[150] Izugbara *et al* 2020: 28.
[151] Ibid.
[152] Pambazuka.org.(2021). The Maputo Protocol: Evaluating women's rights.

security of the person, emphasizing the need for laws to be established and enforced to prohibit all forms of violence against women. Additionally, states are mandated to allocate sufficient financial resources to overcome implementation challenges in combating violence against women.[153]

South Africa, through legislative provisions such as Section 9 of the Constitution as well as through the Domestic Violence Act of 1998 and the Promotion of Equality and Prevention of Unfair Discrimination Act of 2000, among others, creates legislative provisions in line with articles 2,4 and 13 of the Maputo Protocol which protects women against GBV. The shortcoming of the Maputo protocol is that it does not have adequate provisions that relate to cybercrime concerning gender-based forms of cybercrime and women's rights. The protocol does not cater to current enforceability challenges and reporting challenges related to gender-based forms of cybercrimes or any form of solution or guidance for our Cybercrime Act to implement.

V. LEGAL FRAMEWORKS IN SOUTH AFRICA

a. The Constitution of the Republic of South Africa,1996

The Constitution of the Republic of South Africa,1996, serves as the supreme lawof South Africa. It provides the foundational principles and framework for the country's legalsystem. Section 9 of the Constitution states that every citizen is equal before the law and enjoys the right to equal protection and benefit of the law.[154] This provision offers protection against fighting Gender-based Forms of cybercrime through any form of cybercommunication. It does this by enforcing that woman should not be discriminated against, abused, or sexually harassed online because of their race, gender, sex, colour and religion. As enshrined in the Constitution of the Republic of South Africa,1996, the right to equality is fundamental to ensuring fairness and justice for all citizens. This right assert that everyone should be treated equally before the law and have equal access to its protections and benefits.When it comes to gender-based cybercrimes, such as online harassment, stalking, or dissemination of revenge porn, the link to the right to equality is profound. These crimes often target individuals based on their gender, disproportionately affecting women and girls.

The harm inflicted by gender-based cybercrimes is inherently gender-specific, perpetuating stereotypes and reinforcing power imbalances. For example, women and girls are frequently

[153] Ibid.
[154] The Constitution of the Republic of South Africa, 1996.

subjected to online abuse and harassment that is explicitly tied to their gender, such as sexual objectification, threats of violence, or derogatory comments about their appearance or capabilities. This violates their right to dignity and undermines their ability to fully participatein digital spaces without fear of discrimination or harm. In the case of *Bernstein and Others v Bester and Others NNO*, the Constitutional Court emphasized that in South African law, the right to privacy is recognized as an independent personality right incorporated within the concept of *Dignitas*.[155] The court has firmly established the close connection between human dignity and privacy, underscoring the interdependence of these rights.[156] *Financial Mail Pty Ltd and Others v Sage Hodings Limited, and Another* clarified that in cases involving the infringement of personal privacy, the court must delineate the boundary between what is considered offensive and unlawful. This determination should be based on each case's specific circumstances, considering contemporary moral standards and the community's sense of justice.[157] In instances of cyberbullying, the conflicting interests typically involve the right to privacy or dignity versusfreedom of expression. The case of *H, WS, and W, N* highlighted the need for the common lawto evolve, particularly in addressing privacy infringements in social media. The court underscored the deficiency of the common law in handling claims related to cyberspace and reiterated the necessity for developing new legal frameworks.

Moreover, the inadequate response from the state to address gender-based cybercrimes exacerbates the violation of the right to equality. When authorities fail to take these crimes seriously or provide adequate support and protection to victims, it sends a message that such behaviour is acceptable or trivializes the experiences of those affected, disproportionately impacting women and girls. This lack of effective intervention perpetuates a culture of impunity, where perpetrators feel emboldened to continue their abusive behaviour without consequences. In essence, the failure to address gender-based cybercrimes not only violates the right to equality but also perpetuates systemic discrimination and marginalization of women and girls in both online and offline spaces. To uphold the principles of equality and ensure the safety and dignity of all citizens, the state must take proactive measures to combat gender-based cybercrimes, hold perpetrators accountable, and provide support and resources to those

[155] *Bernstein and Others v Bester and Others NN0* 1996 (2) SA 751 (CC) at paragraph 68.
[156] *National Coalition for Gay and Lesbian Equality and Another v Minster of Justice and Others* 1999 (1) SA 6 (CC) where it was said at paragraph (30): This case illustrates how, in particular circumstances, the rights of equality and dignity are closely related, as are the rights of dignity and privacy; and *Khumalo and Others* 2002 SA 401 (CC) at paragraph (21);.
[157] *Financial Mail (Pty) Ltd and Others v Sage Holdings Limited and Another* 1993 (2) SA 451 (A).

affected. A key emphasis is placed on the fundamental principle of "The right to protection and benefitof the law," underscoring the importance of ensuring legal protection and benefits for individuals affected by gender-based cybercrimes. The harsh reality is that it took the government 20 years since the enactment of the Electronic Communications and Transactions Act 25 of 2002 (ECT) to implement a piece of legislation that provides a guarantee to the Constitutional right of protection for women who have been suffering without any right to protection against Gender-Based Forms of Cybercrime. A crucial area for additional research within this topic is the plight of women who have suffered from revenge pornography, wherein their Constitutional right to protection has been compromised due to government inaction.

Section 10 highlights that everyone has the right to protect and respect their dignity.[158] This Constitutional provision, read together with section 10[159] and section 16[160] of the Cybercrimes Act, offers protection concerning gender based forms of cybercrime, explicitly dealing with crimes such as cyber extortion and revenge pornography.

The right to freedom of expression, as outlined in Section 16 of the Constitution of the Republic of South Africa, Act 108 of 1996,[161] is a fundamental principle ensuring individuals can freely express themselves. However, this right is not absolute and is subject to limitations, particularly in forms of expression that incite harm or promote hatred based on specific protected characteristics. In the context of gender-based cybercrimes, some expressions can indeed be viewed as hate speech and thus fall outside the realm of protected freedom of expression. For example, the dissemination of sexual material online with the intent to humiliate, degrade, or incite violence against individuals based on their gender constitutes a clear violation of the right to freedom of expression. Such acts perpetuate harmful stereotypes, objectify individuals, and contribute to a hostile online environment that undermines the safety and dignity of those targeted. In *Van Berg v Coopers and Lybrand Trust (Pty) Limited and Others*, the court emphasized that resolving tensions between Constitutionally protected rights, such as freedom of expression and *Dignitas*, requires a delicate balance.[162] It is crucial to weigh the competing

[158] The Constitution of the Republic of South Africa, 1996.
[159] Any person who unlawfully and intentionally commits or threatens to commit any offence contemplated in section 3 (1), 5 (1), 6 (1) or 7 (1) (a) or (d) of the Cybercrimes Act for the purpose of obtaining any advantage from another person or compelling another person to perform or abstain from performing any act is guilty of the offence of cyber extortion.
[160] Section 16 of the Cybercrimes Act provides that 'any person ("A") who unlawfully and intentionally discloses, by means of an electronic communications service, a data message of an intimate image of a person ("B"), without the consent of B, is guilty of an offence.'
[161] The Constitution of the Republic of South Africa, 1996.
[162] *Van Der Berg v Coopers and Lybrand Trust (Pty) Limited and others* 2011 (3) SA 274 (CC).

interests in a manner that upholds individual rights while considering the broader societal context.

Section 16 of the Constitution explicitly prohibits the advocacy of hatred based on factors such as gender, race, ethnicity, or religion, mainly when it constitutes incitement to cause harm.[163] Therefore, when gender-based cybercrimes involve the spread of incendiary content aimed atvilifying or marginalizing individuals based on their gender, they fall squarely within the realm of prohibited speech under the Constitution. It is crucial to recognize that while freedom of expression is a fundamental right, it does not provide impunity for perpetrators of gender-based cybercrimes to commit acts of harassment, intimidation, or discrimination online. Instead, it places a responsibility on individuals to exercise their freedom of expression in a manner that respects the rights and dignity of others without inciting harm or perpetuating hatred based on gender or any other protected characteristic. While the right to freedom of expression is essential for fostering open discourse and debate, it must be balanced with the need to protect individuals from harm and discrimination, particularly in the context of gender-based cybercrimes. Perpetrators of such crimes cannot hide behind the guise of freedom of expression to justify their actions, as these actions constitute a clear violation of the rights and freedoms of others.

Section 39 stipulates that when interpreting the Bill of Rights, a Court, tribunal, or forum must fulfill several obligations.[164] Firstly, they must promote the values underlying an open anddemocratic society founded on principles of human dignity, equality, and freedom. Secondly, they are required to take into account international law. Lastly, they have the discretion to consider foreign law.[165] This provision in our Constitution underscores the promotion of values essential for fostering an open and democratic society, acknowledging the persuasive influence of international law and foreign legal practices in addressing gender-based cybercrime. By incorporating principles from international legal frameworks and drawing insights from foreign jurisdictions, South Africa can enhance its approach to combating gender-based cybercrimes and align its legislation with global standards and best practices. This approach reflects a commitment to evolving legal norms and ensuring the effectiveness

[163] Ibid.
[164] Ibid.
[165] "When interpreting the Bill of Rights, a Court, tribunal or forum— (a) must promote the values that underlie an open and democratic society based on human dignity, equality and freedom; (b) must consider international law; and (c) may consider foreign law."

of legal responses to emerging challenges in the digital realm.

Engaging in cyberbullying infringes upon multiple rights protected by the South African Constitution. These encompass the rights to freedom of expression, privacy, and dignity, all explicitly outlined in the Constitution.[166] Gender-based cyberbullying violates fundamental rights like freedom of expression, privacy, and dignity, as affirmed by the South African Constitution and reinforced in legal cases, necessitating a robust legal framework to safeguard these rights and hold perpetrators accountable. The act of cyberbullying may lead to a violation of the victim's right to freedom of expression, which can, in turn, encroach upon their rights to privacy or dignity. It is essential to balance these conflicting interests, as emphasized in the *Van Der Berg v Coopers and Lybrand Trust Pty Limited and Others case*.[167]

b. Electronic Communications and Transactions Act 25 of 2002 (ECTA)

According to Watney, cybercrime can be classified as cyber-dependent crimes, cyber-enabled or cyber-assisted crimes, or computer-supported crimes.[168] Importantly, Watney notes that the evolution of ICT legislation in the context of cybercrime has fundamentally been divided into four phases.[169]

In the initial phase, the Internet operated without regulation, resulting in common-law offenses being insufficient to address the intricate methods of cybercrime. The second phase in South Africa commenced with the implementation of the Electronic Communications and Transactions Act (ECTA), substantially improving the efficacy of law enforcement agencies and the criminal justice system in combating cybercrimes. The third phase witnessed the introduction of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) to oversee law enforcement surveillance endeavors.[170] In the *AmaBhungane* case,[171] however, substantial elements of RICA were found to be unconstitutional and unlawful. According to Watney, the fourth phase comprises enacting comprehensive laws addressing cybercrime legislation dealing with issues related

[166] The Constitution of the Republic of South African Act, 1996.
[167] *Van Berg v Coopers*.
[168] Watney cited by S Papadopoulos and S Snail *Cyberlaw @ SA*(2022).
[169] Ibid.
[170] Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
[171] *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC).*

to cybercrime. The application of the Cybercrimes Act[172] in practice was not yet a reality, but several court decisions based on ECTA are examined to illustrate how the courts have tested these provisions and how our Cybercrimes Act can be examined to give order on the practicality of its future use.

The Cybercrimes Act does not replace the Electronic Communications and Transactions Act (ECTA). Instead, it supplements existing legislation by providing specific provisions addressing cybercrime issues. ECTA remains in force and continues to govern electronic communications and transactions, while the Cybercrimes Act focuses specifically on cybercrime-related offences. Therefore, the Cybercrimes Act does not repeal ECTA but complements it to provide a comprehensive legal framework for addressing cybercrimes in South Africa.

Section 85 of the ECTA stipulates that unauthorized access to data or an information system, along with continued access after becoming aware of such unauthorized entry, constitutes an offense. Additionally, Section 86(1) criminalizes hacking or intentional access to a data subject's data or personal information without their consent. Section 86(2) prohibits intentional interference with data to disrupt or render it useless, while Section 86(3) prohibits the manufacture, sale, or distribution of devices intended for circumventing data security measures. Section 86(4) makes it illegal to circumvent copyright security measures, while Section 86(5) prohibits causing a partial or total denial of service. Furthermore, Sections 87, 88, and 89 criminalize cyber fraud, cyber extortion, forgery, and uttering. Violations of the ECT Act's provisions can result in a maximum penalty of an unspecified fine or imprisonment for up to five years.

In *Okundu v S,*[173] the court ruled in favour of an appeal regarding the appellant's sentencing following convictions on several charges under Section 86(1), (3), and (4) of the Electronic Communications and Transactions Act (ECTA). The appellant had been found guilty of unlawfully accessing the information encoded on the magnetic strips of original credit cards issued by multiple banks to different individuals. This access was undertaken without proper authorization or approval from the authorized cardholders or banks.[174]

In the case of *Okundu v. S,*[175] the court determined that the appellant had violated section 86(4) of

[172] Electronic Communications and Transactions Act 19 of 2020.
[173] *Okundu v S [2016] ZAECGHC 131*
[174] *Okundu v S* par 6.

[175] Ibid.

ECTA, which corresponds to section 8 of the Cybercrime Act. This is the fraud provision,and it is vital to pay attention to how the court interpreted it:

Fraud is defined as the unlawful act of making a misrepresentation with the intent to defraud, resulting in actual or potential prejudice to another party. The key elements of fraud include unlawfulness, misrepresentation, causing prejudice or potential prejudice, and intent to defraud. The appellant was convicted on counts 1 to 5 because he unlawfully made misrepresentations to the banks with the intention of defrauding them. These misrepresentations caused prejudice to both the banks and the lawful cardholders involved.[176]

The case highlights the intersection of GBV and cybercrime legislation, with the court applying provisions of the Electronic Communications and Transactions Act (ECTA) and the Cybercrime Act to convict the appellant for fraudulent activities, emphasizing the importanceof legal scrutiny in addressing such offences.

In the case of *Mgoqi v. S*[177] the court granted an appeal and overturned the magistrates' court sentences. The court determined that the appellant had violated section 86(1) of ECTA by illegally and knowingly getting access to or intercepting data, such as client information (encoded on magnetic strips of bank cards) of numerous international financial institutions.[178] Section 3 of the Cybercrimes Act amends this provision of the ECTA.

One of the goals of cybercrime legislation is to prevent the unauthorised overcoming of security measures designed to prevent access to data transmitted to or from a computer system. In the case of *Myeni v. S*[179] the court denied the defendant's appeal after he was found guilty of being a member of a syndicate that predominantly utilised a gadget meant to circumvent security measures. Without permission from the Koukamma Municipality, the criminals used Winspy, a computer program that records keystrokes, to circumvent security measures designed to secure data, especially computer usernames and passwords.[180] The court deemed the punishment imposed by the court a quo appropriate.[181] The case of Myeni v. S exemplifiesthe relevance of cybercrime legislation in addressing elements of gender-based cybercrime particularly unauthorized access to data through circumvention of security measures, as perpetrators utilized a keystroke recording program to breach security protocols and access sensitive information without consent, reinforcing the importance of legal frameworks in combating such offences.

[176] Ibid.
[177] *Mgoqi v S* [2020] ZAECGHC 33.
[178] *Mgoqi v S* supra par 3.
[179] *Myeni v S* [2018] ZAECGHC 107; 2019 (1) SACR 360 (ECG).
[180] *Myeni v S* supra par 4.
[181] *Myeni v S* supra par 29.

The unauthorised and intentional interference with data or a computer programme is prohibited by ECTA section 86(5). S 86(5) of ECTA provides: "A person who commits any act described in this section with the intent to interfere with access to an information system to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence." In *Salzmann v. S,*[182] the SCA determined that a violation of section 86(5) of ECTA is serious. In this case, Cell C, a mobile network provider, suffered a cyberattack at the hands of the appellant. Before dismissing the case, the judge determined:

"Section 89 of the ECTA establishes a maximum penalty of a fine or imprisonment not exceeding five years for a violation of Section 86(5). The inclusion of this offense in the statute highlights the prevalence of unauthorized hacking into others' computers and networks. Such an offense is inherently serious, as it infringes upon the privacy of others, a principle vigorously safeguarded by our legal system, and can have significant consequences. In the current case, the hacking incident affected approximately 80% of the network of a major mobile cellular operator, and it required a week to rectify the damage caused."[183]

The accusation against the appellant was "Importation or Acquisition of Child Pornography."[184] In court, a forensic cyber-analyst, serving as an expert witness, testified that the appellant's computer had been utilized to access child pornography. Additionally, the analyst stated that a software application had been employed to erase child pornography from the appellant's computer mere hours before his arrest.[185] The court rejected the appeal upon scrutinizing the appellant's assertion that third parties had downloaded the child pornography, noting the absence of any provided names of these individuals. Ultimately, the court found the appellant's claim to be fraught with improbabilities and contradictions, leading to the dismissal of the appeal.[186]

The incidents examined briefly illustrate those cybercriminals suffered penalties during the third regulation phase. The ECTA primarily concerns the illegality of interfering with data or information, and as a result, it establishes crimes. From the few publicised cases determined on appeal by the high courts, it is evident that, throughout the years, the lower courts have interpreted and applied section 86 of ECTA to practical scenarios where law enforcement authorities have filed charges against cybercriminals. The court's dismissal of the appeal in

[182] [2019] ZASCA 145; [2020] 1 All SA 361 (SCA); 2020 (2) SACR 200 (SCA).
[183] *Salzmann v S* supra par 40.
[184] *Prinsloo v S* supra par 1.
[185] *Prinsloo v S* supra par 18.
[186] *Prinsloo v S* supra par 45.

Okundu v. S underscores the accountability of cybercriminals under the third phase of regulation, shedding light on how legal frameworks such as the Cybercrimes Act address illicit activities, an aspect I will explore further in my analysis of the Act's provisions.

The legislation lacked specific provisions and mechanisms tailored to combat the growing prevalence of cybercrimes with a gendered dimension. Recognizing the escalating incidents of such offences, the shortcomings of the ECTA prompted amendments to enhance its responsiveness and efficacy in dealing specifically with gender-based cybercrimes. This modification aimed to equip the legal framework with more precise and robust measures to address the unique challenges posed by cybercrimes that disproportionately affect individuals based on their gender. The Act did not cater to nor stipulate that gendered people who are affected by these online cybercrimes can use the Act for recourse and justice.

However, the sections above and examples of case law are clear examples of how we lack the development of adequate "case law" and a process of common law development when dealing with Gender-based forms of Cybercrime. This ultimately reflects upon the lack of consistence in our legal system when dealing with cybercrime forms of GBV due the inadequacy of the ECTA in its failure by only addressing one-half of electronic crimes dealing with economic and financial crimes whereas we have a clear lack for protection for crimes against society, dealing with the surge of online cybercrime forms of GBV. This led to the development and passing of the Cybercrimes Act.

c. The Protection of Personal Information Act 4 of 2013 hereafter referred to as POPIA)

This Act aims to signify advancement in data security standards in South Africa. This Act directly relates to section 14[187] (the right to privacy). The Cybercrime Act uses the definition from POPIA to define personal information. One aspect of the definition of personal information includes any identifying details such as numbers, symbols, email addresses, physical addresses, telephone numbers, and private or confidential correspondence, as well as subsequent communications that disclose the contents of the original communication. In the realm of cyberspace and cybercrime, numerous social media platforms like Instagram, WhatsApp, and email gather personal information. These applications facilitate individual interactions and disclose various details such as photographs, usernames, gender, race, sexual orientation, and marital status. Therefore, all correspondence through social media is protected

[187] The Constitution of the Republic of South Africa, 1996.

in terms of both POPIA and the Cybercrimes Act under the category of personal information.[188]

POPIA establishes principles or rules for the processing of personal information. In the Act, these are referred to as "conditions" for the authorised processing of personal information. Sections 8 and 25 of the Act outline eight conditions: accountability,[189] processing limitation,[190] purpose specification,[191] further processing limitation,[192] information quality,[193]openness,[194] security safeguards,[195] and data subject participation.[196]

In the context of POPIA, the enforcement of rights involves several steps. Firstly, individuals may file complaints. Next, the Information Regulator assesses whether to initiate pre-investigation, conciliatory proceedings, or a full investigation. Complaints may be settled early in the proceedings. If necessary, warrants of entry, search, and seizure may be issued and executed. The Information Regulator evaluates the lawfulness of processing and decides on handling information notices. Matters may be referred to an enforcement committee, and enforcement notices issued. Individuals can lodge appeals in the High Court, and civil remedies may be pursued.[197]

In the context of GBV, the Protection of Personal Information Act (POPIA) plays a crucial role in safeguarding victims' privacy and ensuring accountability for perpetrators. POPIA establishes conditions for the authorized processing of personal information, including accountability, processing limitation, and security safeguards. In enforcing rights related to GBV, individuals can file complaints with the Information Regulator, which may initiate investigations or conciliatory proceedings. The regulator can issue enforcement notices and rely on civil remedies to address violations. This framework protects victims' personal information and facilitates the pursuit of justice in cases of GBV.

In the Constitution, the right to privacy includes the right not to have one's property searched or seized.[198] Musoni examines cyber search and seizure considering both the Cybercrimes Act (with its Bill form at the time of writing) and POPIA. Musoni observes that a search frequently

[188] M De Bruyn, 'The Protection Of Personal Information (POPI) Act - Impact On South Africa.' (2014) *International Business & Economics Research Journal* (IBER).
[189] S 8 of POPIA.
[190] Ss 9–12 of POPIA
[191] Ss 13 and 14 of POPIA
[192] S 15 of POPIA.
[193] S 16 of POPIA.
[194] Ss 16 and 17 of POPIA.
[195] Ss 19–22 of POPIA.
[196] Ss 23–25 of POPIA.
[197] Y Burns and A Burger-Smidt *A commentary on the Protection of Personal Information Act* (2018)

[198] S 14 of the Constitution.

constitutes a severe violation of an individual's right to privacy.[199] In her discussion, Musoni examines judicial precedent on whether the mechanism allowing police officers to utilise warrants to conduct a search and seizure in accordance with the Act is not so vast as to infringe upon the right to privacy arbitrarily.[200] The examination of cyber search and seizure within the framework of both the Cybercrimes Act and POPIA, as discussed by Musoni, sheds light on the potential infringement of individuals' right to privacy, as outlined in the Constitution, particularly concerning GBV cases where the right to privacy is crucial for safeguarding victims' personal information and ensuring accountability for perpetrators.

Musoni first tends to rely on the legal position adopted in *Minister of Safety and Security v Van der Merwe*,[201] where the court ruled that for a search warrant to be deemed valid, it must fulfill certain criteria. These include stating the statutory provision(s) under which it is issued, identifying the searcher, specifying the authority conferred upon the searcher, describing the person, container, or premises to be searched, detailing the article to be searched or seized with adequate specificity, and specifying the type of offense that prompted an external criminal investigation, along with the names of offenders involved.

Musoni critiques the Cybercrimes Act, contending that its breadth allows police officials to conduct arbitrary searches of individuals' emails, social networking profiles, data messages, computer files, and other data forms containing personal information. However, Musoni argues that such searches may encompass information that is not essential or relevant to the criminal investigation at hand.[202] This critique illustrates the necessity for consistency between data protection and cybercrime laws.

[199] M Musoni "Is Cyber Search and Seizure Under the Cybercrimes and Cybersecurity Bill Consistent With the Protection of Personal Information Act?" (2016) *Obiter 6*90.
[200] Ibid.
[201] 2011 (2) SACR 301 (CC) par 55–56.
[202] Ibid.

While both POPIA and the Cybercrimes Act address the gap in data privacy and electronic communication laws, their purposes and goals are distinct. POPIA is intended to protect the data and privacy of entities and specifies a set of minimal rules for data processing in South Africa for this aim. POPIA does not create new cybercrimes but requires organisations to guarantee the integrity of the personal data they process. Nonetheless, there are commonalities in terms of reporting violations and offences. Section 22 of the POPIA mandates that responsible parties notify the Information Regulator of data breaches, and if the breached information renders data subjects identifiable, the data subjects must also be notified. The Cybercrimes Act, on the other hand, mandates reporting by FIs and ECSPs, as described previously.

POPIA and the Cybercrimes Act protect data subjects to improve accountability within South Africa and maybe outside. Before the Cybercrimes Act was enacted, cybercrimes were subject solely to South African common law, exposing data subjects to software hackers and cyber criminals. Incorporating the Cybercrimes Act into South Africa's legislative framework is a critical first step towards enforcing data protection of computer programmes and individuals within our territory.

While POPIA focuses on safeguarding data privacy and imposing rules for data processing, the Cybercrimes Act aims to address gaps in electronic communication laws and combat cybercrimes. Despite their distinct purposes, both legislations share commonalities in reporting violations and offences, enhancing accountability and protection for data subjects. Incorporating the Cybercrimes Act into South Africa's legal framework not only strengthens data protection measures but also provides a critical step in addressing cybercrimes, thereby improving individuals' overall safety and security, including victims of GBV.

d. Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002, hereafter referred to as RICA.

The Constitution guarantees the protection of privacy of communications.[203] Any fundamental right, however, can be limited by a general rule of law if the limitation is reasonable and justifiable in an open and democratic society.[204] RICA is an available applicability Act that allows the provisions of Section 36 of the Constitution to be applied. Any Act that provides for the surveillance and monitoring of communications will, by definition, raise privacy

[203] The Constitution of the Republic of South Africa, 1996.
[204] Section 36 of the Constitution.

concerns. However, given the threat of terrorism and the illegal utilisation of electronic devices, it is argued that such a law is necessary in any modern society, including South Africa.

The objective of RICA is to contribute to enhancing the safety of South Africa. RICA seeks to aid law enforcement agencies in identifying users of mobile phone numbers and tracking criminals who exploit mobile phones for illicit activities.[205] The objectives of RICA make it apparent that while its primary focus is supporting law enforcement authorities in obtaining information needed to combat crime, it also governs interception and monitoring in the private sphere.[206] Section 2 of RICA mandates that no individual may intentionally intercept, attempt to intercept, or authorize or procure another person to intercept or attempt to intercept any communication, whether occurring or in transmission, at any location within the Republic.[207]

With particular focus on the fight against Gender Based forms of Cybercrime and interception by the SAPS of communication of perpetrators, this is governed by Section 45 of RICA: "no person may possess, manufacture, sell or advertise listed equipment – including those which track or obtain information from devices without the targeted person being aware of the act".

In the *Government Gazette*, Lamola stated that acting under section 46 of RICA, and following consultation with Cabinet members responsible for communications, defense, state security, and policing, he has exempted the South African Police Service (SAPS). This exemption permits the SAPS to acquire mass-surveillance equipment for a period of five years.[208]

Lamola asserts that the national police commissioner must personally authorize the acquisitionof various surveillance equipment, including International Mobile Subscriber Identity-catchers (IMSI-catchers) and any necessary accompanying equipment and software. This requirement ensures strict oversight and accountability regarding the procurement and use of IMSI-catchers, which are sophisticated tools capable of intercepting mobile phone signals and tracking individuals' movements. By placing this responsibility on the national police commissioner, it aims to prevent misuse or unauthorized deployment of such surveillance technology, thereby upholding privacy rights and maintaining public trust in law enforcement practices.[209]

---

[205] F Cassim 'Formulating specialised legislation to address the growing spectre of cybercrimes: a comparative study' (2009) 12 *Potchefstroom Electronic Law Journal* 38.
[206] N Bawa 'The regulation of the Interception of Communications and provision of Communication relation information Act' www.thornton.co.za (accessed 14 June 2023), 308.
[207] Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 section 2.
[208] South African government (2023) 184 no. 48627 Government Gazette, 19 May 2023. Available at: https://www.gov.za/sites/default/files/gcis_document/202305/48627rg11584gon3424.pdf (Accessed: 14 June 2023).
[209] Ibid

An IMSI-catcher is a device utilized for eavesdropping on telephone conversations, intercepting mobile phone traffic, and tracking the location data of mobile phone users. It operates as a "fake" mobile tower positioned between the target mobile phone and the service provider's genuine towers. This device is commonly employed in what is known as a man-in-the-middle attack.[210]

Through the exemption, law enforcement is permitted to utilize laser interception devices capable of intercepting direct communications within an effective range of less than 700 meters.[211] Additionally, law enforcement is authorized to utilize miniature radio frequency transmitters capable of intercepting direct communications, as well as miniature recording devices designed for the interception of direct communications. This exemption also encompasses the deployment of miniature video or audio cameras.[212]

From a gender-based form of cybercrime perspective, the decision taken by the minister of State Security to allow such exemptions for the procuring of equipment is a welcomed step in the right direction to combat our fight against gender-based forms of cybercrime The IMSI-catcher can be used as a means of removing anonymity by providing the location data of a possible perpetrator from any location within the country as those who commit gender-based forms of cybercrime often hide behind pseudonyms and fake location markers to mask their identity and location. The efficiency of this device could enhance SAPS investigation procedures, aligning well with the provisions of the Cybercrimes Act on search and seizure, wherein a warrant may be issued if it appears that the article in question is located within the Republic. However, the specific jurisdiction where it is being used or involved in the commission of an offence is unclear."[213] With equipment such as the IMSI-catcher, SAPS investigators will be able to keep up to date with changing forms of technology, pinpoint the location data of the mobile user and apply for a warrant in terms of S 29(1)(a)(ii)(bb) of the Cybercrimes Act.

e. Protection from Harassment Act 17 of 2011

[210] A Moyo (2023) Police given power to intercept cellular communications, ITWeb. Available at: https://www.itweb.co.za/content/KA3Ww7dzBBkqrydZ (Accessed: 14 June 2023).
[211] Ibid.
[212] Ibid.
[213] S 29(1)(a)(ii)(bb) of the Cybercrimes Act.

South Africa's legislature adopted the Protection from Harassment Act[214] in 2011 in response to the widespread scourge of harassment against individuals of all ages and backgrounds, including vulnerable groups such as women, children, and marginalized communities, The Protection from Harassment Act 17 of 2011 was enacted to offer protection, provide legal recourse, and prevent further harm through accessible and enforceable legal measures. The Act seeks to protect fundamental rights such as equality, privacy, dignity, freedom and security of persons.[215]

While the Act was adopted with traditional forms of harassment in mind, it did not sufficiently cater for emerging trends such as technologically facilitated harassments, which constitutes gender-based forms of cybercrimes. In their criticism of the Act, Batchelor and Makore note that "Equally, such maximum protection can only be achieved when the Act addresses not only traditional forms of harassment but also non-traditional forms of cyber-related abuse that can occur through digital technology and other social media platforms."[216] Scholars indicate that "classification is based on the nature of the perpetrator's conduct and the space in which the conduct occurs. This binary delineation is implicitly alluded to in the Act and is significant for the purpose of effectively combating all types of harassment."[217]

Gender-based forms of cybercrimes has become increasingly prevalent and aggressive due to the continuously expanding nature of digital platforms. These platforms allow for a wide reach, where harassers can target individuals quickly and often anonymously. The anonymity and lack of physical presence make it easier for perpetrators to act without immediate consequence, often leading to more extreme behaviour. Additionally, the permanence and widespread dissemination of harmful content online can exacerbate the trauma for victims, making recovery more challenging.

The Act acknowledges that harassment can occur through email communication.[218] An email can be defined as "a way of sending messages and data to other people by means of computers connected together in a network".[219] This definition is broad enough and can be extended to include all forms of cyberspace communication. Gender-based forms of cybercrimes often occur across unrestricted computer networks, which can be accessed by numerous devices, not limited to computers alone. These crimes frequently involve cell phones, which today function as portable computers.

[214] Protection from Harassment Act 17 of 2011.
[215] Arndt "Street Harassment: The Need for Criminal Remedies" 2018 29 Hastings Women's Law Journal 81.
[216] BLA Batchelor, and ST Mota Makore, 'Combating harassment under the protection from harassment act 17 of 2011 in South Africa: Does it punish victims and protect perpetrators?' (2021) 42 (2) Obiter, pp.269-288. 270.
[217] Ibid.
[218] Cassim "Formulating Adequate Legislation to Address Cyber-Bullying: Has the Law Kept Pace with Advancing Technology?" 2018 26 South African Computer Journal 4.
[219] E-mail noun - definition, pictures, pronunciation and usage notes | oxford advanced american dictionary at Oxfordlearnersdictionaries.com. Available at: https://www.oxfordlearnersdictionaries.com/definition/american_english/e-mail_2 (Accessed: 04 September 2024).

The Act allows for the court to issue an order for an electronic communications service provider to provide details of an alleged harasser or may order an investigation by the police to obtain the details of the alleged harasser.[220] The Act offers protection against electronically communicated harassment by means of a court order outlining the details of an alleged harasser.[221] If the court is satisfied that a protection order should be issued but the identity of the electronic harasser is unknown, the court may direct a service provider to provide the harasser's information.[222] The gathering of this information must comply with section 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICPCI).[223] This development by the Act is a positive step forward, as it provides victims of gender-based forms of cybercrimes with some relief by enabling the tracing of alleged unknown perpetrators. The court's authority to direct service providers and law enforcement to conduct thorough investigations and disclose the details of alleged harassers serves as a deterrent to individuals who might use technology to commit such offenses and offer victims with practical support.

Once an interim order has been granted, it must be served, which may require mobile operators and Internet service providers (ISPs) to help locate the involved parties. Service providers can be compelled to disclose the name, surname, identity number, and address linked to an IP address, email, or phone number. ISPs that fail to provide the required information may face fines of up to R10,000, and their staff could be subject to six months of imprisonment.[224] Service providers are required to either provide the necessary information or indicate that they do not have it within five court days. Additionally, at least 48 hours before supplying the information to the court, the service provider must notify the respondent about what information will be provided.[225] Failure to comply with these requirements constitutes a criminal offense under the Act. This development represents a positive step forward in the fight against Gender -based forms of cybercrime, as it ensures accountability for non-compliance with orders that compel service providers to provide such information.

The Act addresses the practicalities of imposing such orders through guidelines for service providers, including the timeframe for the release of information and the challenges of dealing with perpetrators who are anonymous or have used false documents for SIM card registration. Additional to establish training protocols for the South African Police Service (SAPS), the need for updated technological

[220] Bick "SA's New Harassment Act Explained" (22 April 2013) http://www.women24.com/CareersAndMoney/Legal/SAs-new-Harassment-Act-explained-20130422T (accessed 2014-06-16).
[221] Ibid
[222] Landman and Ndou 2013 22 Contemporary Labour Law 83.
[223] 70 of 2002.
[224] S 18(4)(b) of the Act.
[225] S 18(4)(a) of the Act.

equipment to combat such offences and specialised training for prosecutors on implementation of such cases on the court role.

The Act provides victims with remedies that were previously inaccessible due to financial constraints or rigorous requirements. It establishes a framework that simplifies the process of obtaining a protection order and a suspended warrant of arrest, thereby safeguarding the complainant's fundamental rights and achieving the objectives of the Act. Before the enactment of the Protection from Harassment Act, protection orders were only available under the Domestic Violence Act (DVA)[226] to individuals experiencing physical, sexual, emotional, verbal, psychological, economic, or other forms of abuse from someone with whom they had a domestic relationship.

This meant that applicants could only seek a protection order against a spouse, fiancée, or someone with whom they were in a romantic, intimate, or sexual relationship, as well as against a parent, child, family member, or cohabitant. In contrast, the Protection from Harassment Act allows individuals to obtain a protection order without needing to prove the existence of a domestic relationship, which serves as a significant improvement, as victims of gender-based forms of cybercrimes often do not know who the perpetrators of offences are and often times it includes individuals who are not in a domestic relationship with the alleged perpetrators. This removes a significant barrier to obtaining protection orders, particularly in cases of harassment or abuse that occur outside of domestic relationships.

It can thus be argued that the Protection from Harassment Act 17 of 2011 provides protection against cybercrimes that involve harassment, however much more can be done to implement stricter provisions to include gender-based forms of cybercrimes.

VI. CONCLUSION

In conclusion, the analysis of international and legal frameworks presents a comprehensive strategy to tackle gender-based forms of cybercrimes. Fundamental international conventions, notably the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW), demonstrate a commitment to addressing technology-related violence against women. CEDAW, often considered a global milestone for women's rights, recognises explicitly online and technology-facilitated violence, providing a foundation for national measures combating GBV, including in cyberspace. The Beijing Declaration and Platform for Action emphasize the transformative agenda for women's involvement in media and technology, shedding light on persistent challenges in countering gender-based cyber violence. The International Covenant on Economic, Social and Cultural Rights indirectly contributes

[226] Domestic Violence Act 116 of 1998

to overall well-being, influencing vulnerability to cybercrimes and highlighting the interconnectedness of human rights and cyberspace challenges.

However, limitations are observed, particularly in the Council of Europe Convention on Cyber Crime and regional protocols like the Maputo Protocol and the SADC Protocol on Gender and Development. The analysis underscores the need for continuous adaptation of these frameworks to address emerging forms of gender-based cybercrimes effectively. The chapter emphasized the importance of harmonizing legal approaches across Africa, pointing to the significance of South Africa's ratification of the Malabo Convention. In essence, it calls for a holistic and intersectional approach, recognizing the dynamic nature of technology and the evolving landscape of cybercrimes, emphasizing the ongoing necessity to strengthen legal mechanisms and foster international cooperation in tackling this complex challenge.

Constitutional provisions and existing legislation underscore the multifaceted approach required to address gender-based cybercrimes within South Africa's legal framework. Ensuring compliance with Section 9 of the Constitution, which guarantees equal protection under the law, mandates proactive measures to combat cybercrimes targeting women and girls. Additionally, the application of Section 16 highlights the delicate balance between freedom of expression and protection from harmful speech, particularly in cases of gender-based cyberbullying. By incorporating international law and considering foreign law best practices, as stipulated in Section 39, South Africa can strengthen its legal response to gender-based cybercrimes and uphold the rights to privacy, dignity, and freedom of expression for all individuals

CHAPTER THREE: THE SALIENT PROVISIONS OF THE CYBERCRIMES ACT

I. INTRODUCTION

This chapter is dedicated to exploring the salient provisions within the Cybercrimes Act. In alignment with the overarching research question guiding this study, the primary objective of this chapter is to scrutinize and analyze the specific legal facets encapsulated within the Cybercrimes Act. The significance of this examination lies in its contribution to a nuanced understanding of the Cybercrimes Act and its implications within the broader context of the study. This analysis is pivotal for discerning the legislative responses to cybercrimes, their efficacy, and their potential impact on the broader cybersecurity landscape.

In 2021, South Africa enacted the Cybercrimes Act 19 of 2020[227], a legislative initiative spearheaded by President Cyril Ramaphosa. The Act does not replace the Electronic Communications and Transactions Act (ECTA) but supplements it by addressing specific aspects of cybercrime within South Africa's legal framework. This law was designed to address various aspects of cybercrime, including the criminalization of harmful data message disclosure, the establishment of offences related to cybercrime, the provision of interim protection orders, and the further regulation of jurisdiction, investigative powers, and mutual assistance concerning cybercrimes.[228] While the legislation plays a pivotal role in safeguarding the dignity of women from practices like gender trolling, threats, and image-based sexual abuse, it does not explicitly address Gender-Based forms of Cybercrime against women and girls. Instead, it broadly refers to online violence against individuals or groups without specific gender-based distinctions.[229]

The Cybercrimes Act is of paramount importance as it aims to counter the escalating growth of cybercrimes, offering protection against criminals, cyber extortionists, and online users who exploit the anonymity of the internet.[230] This legislation consolidates cybercrime laws into a unified framework, emphasizing its primary objective to combat cybercrimes and

[227] The Cybercrimes Act 19 of 2020.
[228]S Snail ka Mtuze, and M Musoni, 'An overview of cybercrime law in South Africa.' (2023) 4 *Int. Cybersecur. Law Rev* 299–323 .
[229] Ibid.
[230] F Cronje, S Snail, AOlivier, J and Jordaan . *The Cybercrime Act—What you need to know* (2022) 3–4.

enhance the nation's online security, particularly by criminalizing the disclosure of harmful data messages. This legislation's origins can be traced back to the first cybercrimes and cybersecurity Bill in 2015, subsequently amended in 2017. The preamble of the Cybercrimes Act 19 of 2020 articulates its objectives, focusing on creating offences relevant to cybercrime and prescribingpenalties for such actions.[231]

The legislation comprises nine chapters. In Chapter 1, definitions and interpretations are provided. Chapter 2 covers various cybercrimes, malicious communications, sentencing, and orders to safeguard complainants from the harmful effects of malicious communications. Jurisdictional matters are addressed in Chapter 3. Chapter 4 outlines the powers granted to law enforcement agencies for investigation, search, access, or seizure. Mutual assistance between South Africa and foreign states is explained in Chapter 5. Chapter 6 establishes and delineates the functions of a 'designated point of contact.' Chapter 7 outlines provisions for presenting evidence through sworn statements. Chapter 8 imposes obligations on electronic communications service providers and financial institutions to report cybercrime offences and preserve relevant information for investigations. Finally, Chapter 9 includes general provisions covering the authority of the executive office to enter into agreements, the repeal and amendment of specific laws, the inclusion of regulations, and the commencement of the Act.[232]

II. ANALYSIS OF RELEVANT PROVISIONS PERTAINING TO GBV FORMS OFCYBERCRIMES

a. Offences against confidentiality, availability, and integrity of data

Part I of Chapter 2 of the Cybercrimes Act outlines various forms of cybercrime offences. The Cybercrimes Act does not furnish a self-contained definition of cybercrime. Instead, it delineates specific components integral to the cybercriminal landscape, such as the characterization of a computer device, the nature of data, and the types of conduct falling under the classification of accessing a computer or network.[233] The desirability of a singular definition

[231] S Snail 'Legal Intersections between the Protection of Personal Information Act 4 of 2013 (POPIA) and the Cybercrimes Act 19 of 2020' (2001) https://cyberbrics.info/legal-intersections-between-the-protection-of- personal-information-act-4-of-2013-popia-and-the-cyber-crimes-act-19-of-2020-2/

[232] S Snail 'The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' 2022 *Obiter Law Journal* 536 at 544.

[233] SM Mabunda "The South African legislative response to cybercrime" LLM dissertation. University of Western Cape (2021).

of cybercrime is a highly debated subject among scholars and practitioners, primarily due to the intricate nature of cybercrime. Notably, a computer or device can serve as an agent,facilitator, or target of a crime. Additionally, the commission of the crime may occur either on the computer itself or in a non-virtual location.

The subsequent analysis delves into the offences explicitly outlined and criminalized by the Cybercrimes Act. These include unlawful access (section 2), unlawful interception of data (section 3), unlawful acts concerning software or hardware tools (section 4), unlawful interference with data or computer Programmes (section 5), unlawful interference with computer data storage mediums or computer systems (section 6); unlawful acquisition, possession, provision, receipt, or use of a password, access code, or similar data or device (section 7); cyber fraud (section 8); cyber forgery and uttering (section 9); cyber extortion (section 10); and theft of incorporeal property (section 12). This analysis will critically examine these offences, considering their relevance and applicability to gender-based cybercrimes while highlighting gaps or concerns within this context.

i. Unlawful access

Section 2 of the Act pertains to offenses concerning unlawful access. Under this section, an individual commits a cybercrime if they intentionally and unlawfully engage with a computer system or data storage medium, thereby positioning themselves or another person to commit an offense. Furthermore, section 2 prohibits unauthorized access to a computer system or datastorage medium.[234] The section clarifies how to access or store data or a computer program ona computer data storage medium.[235] The section emphasizes that accessing a computer system encompasses a range of actions, such as utilizing data or a computer program within the system, storing data or a program on a computer data storage medium within the system, or giving instructions, communicating with, or otherwise employing the computer system.[236] The section outlines that a person is considered to be using a computer program if they can move or copythe program to a different location, cause a computer program to execute any function, or obtain the output of a computer program.[237]A person uses data if this person copies or moves the data to a different location or obtains

[234] Section 2 (2) (a) of the Cybercrimes Act.
[235] Section 2 (2) (b) (i) of the Cybercrimes Act.
[236] Section 2 (2) (b) (ii) of the Cybercrimes Act.
[237] Section 2 (2) (c) (i) of the Cybercrimes Act.

the output of data. Section 2 addresses unauthorized access to computer systems. It identifies an offence as knowingly and unlawfully gaining access to data, a computer program, a computer data storage device, or a computer system. This statement suggests that although the given definition encompasses the idea of unauthorized access, it lacks specificity and comprehensive safeguards for individuals who are victims of Gender-based forms of Cybercrime. This inadequacy is particularly notable given the rising prevalence of such cybercrimes in the digital era.

The current wording of Section 2, which pertains to unauthorized access to computer systems, lacks explicit consideration of critical issues related to GBV forms of cybercrime. This omission leaves victims susceptible to harm, as it fails to adequately address the specific nature of cybercrimes that target individuals based on their gender. The section does not encompass the unique dynamics and harm associated with GBV in the cyber realm. This oversight raises concerns about the potential for perpetrators to evade suitable legal consequences, as the existing language does not effectively capture the nuances and gravity of GBV-related cybercrimes. Consequently, there is a notable gap in the protection of victims and the prosecution of offenders within the current framework of Section 2. If attuned to these issues, state authorities would need to address and rectify these gaps to ensure a more comprehensive legal response to GBV forms of cybercrime.

The revision of Section 2 is essential to ensure a more inclusive and comprehensive scope that adequately addresses all manifestations of computer access. Specifically, there is a crucial need for explicit acknowledgement of Gender-based forms of Cybercrime within the concept of "unlawful access." Currently, the wording falls short of capturing the diverse range of cybercrimes that may disproportionately target individuals based on their gender. For instance, cybercrimes such as online harassment, cyberstalking, or the unauthorized distribution of intimate images often disproportionately affect women and contribute to the broader landscape of GBV in the digital sphere. By refining the language of Section 2 to recognize and encompass these gender-specific cybercrimes explicitly, the law can better protect victims and facilitate the prosecution of perpetrators, addressing a significant gap in the legislation's ability to combat Gender-based forms of Cybercrime effectively..." By incorporating such language, the act would demonstrate a firm commitment to protecting individuals, especially women, from the harmful effect of these heinous offences.

ii. Unlawful interception

Section 3 of the Cybercrimes Act delineates three prohibited conducts: Firstly, it prohibits illegal and intentional data interception,[238] exemplified by the unauthorized cloning of a Visa debit card to obtain data encoded on its magnetic strip. Secondly, it criminalizes the illegal and intentional possession of intercepted data,[239] even by individuals who did not commit the initial interception but are aware of the data's illegal origin. Thirdly, the Act prohibits possession of data under circumstances suggesting unlawful interception,[240] where individuals fail to provide a satisfactory explanation for their possession of such data. These provisions aim to deter cybercriminal activities, safeguard data integrity, and promote accountability within the digital realm.

Within Section 3 of the Act, an infringement is delineated as the unauthorized interception of data, encompassing activities such as wiretapping, installing a sniffer to monitor network traffic, and packet sniffing. These actions represent violations that compromise the confidentiality and security of digital communications. Wiretapping involves the unauthorized interception of telecommunication signals while deploying a network sniffer, which allows for the clandestine monitoring of data flowing through a network. Additionally, packet sniffing entails the unauthorized capture and analysis of data packets transmitted over a network. Section 3, therefore, targets a range of intrusive practices that compromise the integrity of digital communications, contributing to the legislative framework's efforts to address and deter unauthorized interception of data.[241]

While a sniffer is described as an ‘application that monitors data delivered through a network,’ wiretapping uses electrical equipment to observe conversations between two different computers.[242] Watney clarifies that monitoring involves "the listening to and reading of communication content," adding precision to the interpretation of technical terms. In contrast, surveillance is described vaguely and generally as "to watch over." This distinction is crucial in Section 3's exploration, as it underscores the focus on unauthorized interception of data, which aligns more closely with the detailed actions involved in monitoring rather than the broader and less specific notion of surveillance. By drawing on Watney's definitions, the analysis gains depth, aiding in a clearer understanding of the legislative intent and contributing to a more precise interpretation of Section 3 within the broader framework of cybercrime

[238] Section 3 (1) of the Cybercrimes Act.

[239] Section 3 (2) of the Cybercrimes Act.
[240] Section 3 (3) of the Cybercrimes Act.
[241] SM Maat Cybercrime *Unauthorised Interception* (2009) See also Van der Merwe *Computers and the Law* (2000) 169; and Gordon “Internet Criminal Law” in Buys (ed) Cyberlaw @ SA (2000) 428.
[242] Ibid.

legislation. Clarity in interpreting Section 3 is paramount, necessitating considering extant research and legal frameworks, notably the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA). When technical terms, such as "monitor," lack explicit definition within the Act, consulting related legislation becomes imperative. For instance, RICA defines "monitor" as listening to or recording communication through monitoring equipment.

This cross-reference aids in establishing a more precise understanding of the technical terminology employed in Section 3, contributing to a comprehensive and legally sound interpretation of the provision. Individuals experiencing gender-based forms of cybercrime may be susceptible to perpetrators intercepting their personal information and subsequently posting it online without their explicit consent. This violation has a gendered dimension, particularly when considering the prevalence of cybercrimes such as doxxing or the non-consensual distribution of intimate images that disproportionately target women. The act of intercepting and disseminating personal information in this manner not only infringes upon privacy rights but may also contribute to the perpetuation of gender-based harm, reinforcing the need for specific legal provisions to address and prevent such gendered forms of cybercrime.

From a gender perspective, the vulnerability associated with intercepting and disseminating personal information, particularly concerning minors, manifests as an increased risk of manipulation and exploitation. Minors, who are already in a more susceptible position due to their age, become especially vulnerable to cyber threats when their personal information is intercepted and used without consent. This vulnerability is exacerbated by the ease with which perpetrators can manipulate and threaten minors, subjecting them to potential exploitation. In the context of gender-based cybercrimes, this heightened vulnerability underscores the need for targeted legal safeguards and interventions to protect minors, significantly when their personal information is compromised, to mitigate the risks of manipulation, exploitation, and potential long-term harm.

Due to the instability of data, it is very conceivable for third parties to obtain material that has been improperly intercepted. This provision appears to have been added by the legislature to restrict further access and use of such data. The stipulation that a third party possessing intercepted data must offer a sufficient explanation for acquiring such data has significant implications for the study. This provision could aid in identifying potential intermediaries involved in the unauthorized interception of personal information, contributing to

understanding the dynamics of cybercrimes. It may assist in uncovering the chain of events leading to the interception, shedding light on the roles of different actors in committing these offences. However, potential gaps or critical issues may arise if the Act does not specify the criteria or standards for what constitutes a "sufficient explanation." The lack of clarity in this regard could pose challenges in assessing the legitimacy of third-party explanations and may warrant further investigation to ensure the effectiveness of the legal framework in addressing gender-based cybercrimes.

iii. Unlawful acts

Section 4 of the Cybercrimes Act criminalises any conduct using software or hardware instruments for unlawful access, unauthorised interception, or unauthorised interference.[243] The offence of unlawfully and intentionally acquiring, possessing, providing to another person, or using a password, an access code, or similar data or device to violate the provisions of sections 2 (1) or (2), 3 (1), 5 (1), 6 (1), 8 or 9 (1) of the Cybercrimes Act creates an infringement in terms of section 4 of the Act.[244]

Section 4 introduces a noteworthy element by criminalizing the utilization of specific software or hardware tools and the mere possession of such tools. This provision serves as a safeguard against individuals who seek to exploit digital tools to create, distribute, display, or produce sexual content without consent, with the explicit intention of inflicting severe emotional and physical harm upon the targeted individuals.

In the context of Gender-based forms of Cybercrime, where individuals, particularly women, are disproportionately targeted, this clause potentially can serve as a deterrent against the exploitative use of digital material to degrade and exploit individuals. The gendered nature of vulnerability in this context is primarily associated with the heightened risk of gender-based exploitation. When personal data, incredibly intimate or private information, is intercepted and possessed by a third party, vulnerable individuals, particularly women and minors, become susceptible to exploitation. This may include the non-consensual distribution of intimate images or the use of personal information for manipulative purposes. The proper application of the provision requiring a third party to provide a sufficient explanation for possessing such data could significantly assist in addressing gender-based cybercrimes. By scrutinizing the purpose behind the possession of these tools, law enforcement can identify instances where

[243] Section 4 Cybercrimes Act.
[244] Section 7 (1) Cybercrimes Act.

personal information is acquired and held for malicious intent, helping to mitigate the gendered impacts of cybercrimes and providing a legal basis for prosecuting those involved in such exploitative practices. In conclusion, Section 4 introduces a distinctive and crucial legal argument by criminalizing the utilization and possession of software or hardware tools for illicit purposes. This provision's implications extend to Gender-based forms of Cybercrime, as it presents a formidable barrier against disseminating explicit and harmful content.

iv. Unlawful interference

Section 5 of the Cybercrimes Act outlines offenses related to interference with data or computer programs. The Act provides clarification on the definition of "interference," which encompasses various actions. These actions include deleting, altering, making vulnerable, damaging, deteriorating, rendering meaningless, useless, or ineffective, obstructing, interrupting, or denying access to data or a computer program.[245] Section 6 of the Cybercrimes Act stipulates that an interference has transpired when there is either a permanent or temporary alteration of any resource, or an interruption or impairment to the functioning, confidentiality, integrity, or availability of a computer data storage medium or a computer system.[246]

The Act explicitly covers a broad spectrum of conduct to afford victims of gender-based cybercrimes enhanced protection. This includes situations where potential perpetrators may attempt to tamper with computer systems to permanently alter, interrupt, or impair their functioning and the associated information used in committing the crime. The gendered nature of vulnerability in this context, particularly affecting women who are often targeted in gender-based cybercrimes, underscores the significance of this provision. By addressing potential interference with computer systems, the Act serves as a deterrent against malicious actions that exploit gender vulnerabilities. Moreover, this provision acts as a valuable tool for prosecuting offenders who engage in activities that compromise the integrity of computer systems and perpetuate gender-based cybercrimes. The legislature's carefully crafted definition of "interference" is anticipated to provide the courts with legal certainty when dealing with diverse cyber-interferences.

Watney's assertion that communication on the Internet involves a right to privacy underscores a crucial aspect of digital interactions. Her emphasis on communications privacy as a defence

[245] Section 5 (2) of the Cybercrimes Act.
[246] Section 6 (2) of the Cybercrimes Act.

against interference and intrusion aligns with established privacy principles in online spaces. This perspective is particularly relevant to the study and argument, as it accentuates the significance of safeguarding individuals' privacy in the context of cybercrimes, including gender-based forms. Recognizing communications privacy as a defence speaks to the need for robust legal measures to protect against unwarranted intrusion and interference in online communications. This aligns with the argument that the legal framework should address not only the overt acts but also the underlying violations of privacy that characterize many gender-based cybercrimes. Watney's stance contributes to a broader understanding of the importance of privacy in the digital realm, reinforcing the relevance of privacy considerations in the study of cybercrime legislation, particularly concerning gender-based cybercrimes.[247]

b. Malicious computer-related crimes- Sections 7, 8, 9 and 10 of the Act

i. Cyber Fraud

This cybercrime is commonly found in “phishing” and “spoofing”. "Phishing" and "spoofing" are both cybercrime techniques aimed at deceiving individuals for malicious purposes. Phishing involves perpetrators attempting to trick individuals into disclosing sensitive information, such as login credentials or personal details, by posing as trustworthy entities. This is often executed through deceptive emails, messages, or websites that mimic legitimate sources, creating a false sense of trust and urgency to prompt recipients to reveal confidential data. On the other hand, spoofing entails creating deceptive elements, like email addresses or websites, to masquerade as a trusted or legitimate source. The primary objective of spoofing is to deceive users, gain unauthorized access, distribute malware, or conduct phishing attacks. For instance, email spoofing involves forging the sender's address to appear as if the message comes from a trustworthy source, aiming to manipulate recipients into taking specific actions.[248] To address emerging methods of committing fraud, the Cybercrimes Act incorporates provisions for a specific type of fraud involving data and computer Programmes. Section 8 of the Cybercrimes Act delineates that any individual who unlawfully, with the intent

[247] M Watney “The Evolution of Internet Legal Regulation in Addressing Crime and Terrorism” (2007) 2 *The Journal of Digital Forensics, Security and Law* 40.

[248] The former activity entails sending out an e-mail purporting to require information from the recipient for some legitimate purpose in the form of a request for personal details, e.g. for a bank account. Sometimes these messages direct the recipients to a “spoof” false website, usually a website controlled by the criminal purporting to be a legal website—again usually resembling that of a genuine bank. After having acquired the personal information, the identity thief can gain access to the victims through banking or shopping
online channels and fraudulently purchase goods and services

to defraud, makes a misrepresentation using data or a computer program, or through interference with data or a computer program, or interference with a computer data storage medium or a computer system, resulting in actual or potential prejudice to another person, commits cyber fraud.[249] The relevance of Section 8 of the Cybercrimes Act to gender-based cybercrime lies in its potential applicability to cases involving misrepresentation through the use of data or computer Programmes. This section becomes pertinent when perpetrators exploit deceptive tactics, such as phishing or social engineering (common methods in gender-based cybercrimes), to defraud individuals. However, there might be gaps in explicitly addressing gender-specific cyber fraud or misrepresentation in the legislation. A nuanced understanding of the unique tactics and motives involved is crucial to combat gender-based cybercrime. While Section 8 provides a legal basis to address cyber fraud broadly, further refinement or explicit inclusion of gender-specific elements could enhance its utility in combating gender-based cybercrimes. Overall, Section 8 serves as a valuable tool in addressing specific aspects of cyber fraud, but its effectiveness in addressing the gendered nature of cybercrime could be augmented with more explicit considerations.

The argument that the Cybercrimes Act might be redundant in addressing cyber fraud because it could be prosecuted under common law warrants consideration. While standard law provisions might cover cyber fraud to some extent, including specific legislation, such as the Cybercrimes Act, brings unique advantages. Specialized laws can offer clarity, precision, and updated definitions tailored to the dynamic nature of cybercrimes. In the context of gender-based cybercrimes, explicit provisions in the Cybercrimes Act can contribute to a more comprehensive legal framework. Such provisions can address the nuances of gendered cybercrimes, providing a more precise legal basis for prosecution. Therefore, while common law might offer a foundation, specialized legislation like the Cybercrimes Act can enhance the legal response to cyber fraud, especially in cases with gender-specific elements, reinforcing the value of its inclusion in the argument. Mabunda argued that a crime such as cyber fraud is notan actual cybercrime, and the mere presence of an internet element in committing fraud is insufficient to elevate the crime to cyber fraud status. This argument stems from the transformational test that an actual cybercrime will cease to exist if we take away computers and the internet.[250]

[249] Section 8 of the Cybercrimes Act.
[250] Mabunda op cit at 58.

ii. Cyber forgery and uttering

Cyber forgery is the illegal and purposeful falsification of data or a computer program to another person's actual or potential disadvantage.[251] Cyber uttering is delineated as the deliberate and unlawful dissemination of false data or a fabricated computer program, with the genuine or potential consequence of causing harm to another individual. [252] The Cybercrimes Act distinguishes common law offences such as fraud, forgery, and extortion by linking them directly to the use of data and a computer or computer programme.[253] As a result, it is assumed that the scope and application of the Cybercrimes Act in connection to these offences appear to be well-fitted for the context of crimes committed in conjunction with data and computers.[254] The statement suggests that the Cybercrimes Act is presumably well-suited to address offences related to data and computers, such as cyber uttering. Analyzing these provisions implies that the Cybercrimes Act provides a suitable legal framework for prosecuting offences related to data and computers, particularly relevant to studying gender-based cybercrimes. However, a more nuanced examination is necessary to determine how effectively the Act addresses the gendered nuances within these cybercrimes and whether there are specific provisions that might need refinement or expansion to address gender-based offenses in the digital realm comprehensively.

iii. Cyber extortion

Any person who unlawfully and intentionally commits or threatens to commit any offence contemplated in sections 3 (1), 5 (1), 6 (1) or 7 (1) (a) or (d) of the Cybercrimes Act to obtain any advantage from another person or compelling another person to perform or abstain from performing any act is guilty of the offence of cyber extortion.[255] While this provision addresses extortion in a broad sense, it may not explicitly encompass the gendered nuances inherent in

[251] Section 9 (1) of the Cybercrimes Act.
[252] Section 9 (2) of the Cybercrimes Act.
[253] For example, in *Van Heerden v S (A160/2016) [2016] ZAFSHC 191*, the Court gave the Common Law definition of fraud by stating that, *"Fraud is the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another."* See *Hattingh v S* (A307/2015) [2016] ZAWCHC 199 in respect of the Common Law definition of forgery; Ndlovu v S (CA&R14/2016) 2016 ZAECBHC 12 for a characterization of the Common Law crime of extortion; and Cossie v S (A114/2011) [2011] ZAFSHC 169 in respect of the Common Law crime of uttering.
[254] Snail op cit at 550.
[255] Section 10 of the Cybercrimes Act.

certain cybercrimes. The language and scope of the provision necessitate a more nuanced analysis to determine its effectiveness in addressing gender-specific cyber extortion, thus highlighting potential gaps in the Act's ability to tackle gender-based cybercrimes comprehensively.

iv. Aggravated offences

Section 11 of the Cybercrimes Act provides for aggravated offences and explains that its application includes sections 3 (1), 5 (1), 6 (1), and 7 (1) insofar as passwords, access codes, or similar data and devices are involved.[256] In this case, the responsibility of guilt attached to an infringer/perpetrator is strict in that such a person may be held guilty of an aggravated offence if he or she knows or ought reasonably to have known/suspected that the computer system is restricted.

Furthermore, the perpetrator is guilty of an aggravated offence if he or she knows or should reasonably have known or suspected that the offence in question will (a) endanger the life or cause serious bodily harm or death to any person or any number or group of persons, (b) endanger the health or safety of the public or any segment of the public, or (c) create a public severe emergency."[257]

The Cybercrimes Act takes a strong stance against cybercrimes, holding perpetrators strictly liable for knowingly engaging in prohibited conduct or reasonably suspecting the consequences. It establishes aggravated offences for actions endangering lives, public health, and safety or causing emergencies, demonstrating the Act's recognition of the seriousness of cybercrimes. This legal framework fosters accountability and serves as a deterrent against cybercriminal activities.

v. Theft of incorporeal property

In terms of Section 12, “the common law offence of theft must be interpreted not to exclude the theft of an incorporeal object. Section 12 states that "the common law offence of theft must be understood so as not to exclude the theft of incorporeal property.” It is a rather simple and

[256] Snail, op cit at 550.
[257] S 11 of the Cybercrimes Act.

understandable provision. As a result, this rule mandates that the theft of incorporeal property is a common-law "theft" offence.[258]

In the analytical assessment of Sections 7-12, the focus primarily revolves around cybercrimes that have undergone amendments from pre-existing statutes. The prima facie perspective generated by the examination suggests that the Cybercrimes Act is well-aligned with the context of offences associated with data and computers. This initial impression, derived fromthe Act's provisions, indicates a seemingly appropriate fit for addressing crimes in the digital realm. However, a more comprehensive examination is warranted to ascertain how effectivelythe Act addresses the intricacies of gender-based cybercrimes within this framework.

These sections do not address the issue of Gender-based forms of Cybercrime. As a result, sections 7-12 of the Cybercrimes Act are insufficient for addressing Gender-based forms of Cybercrime. These sections deal with crimes such as hacking, defined as unauthorized and illegal access to data stored on a data storage device. When someone defrauds another person by creating or passing-off false data, this is called cyber forgery and uttering. Cyber extortion occurs when criminals threaten to disable and compromise the accessibility and confidentiality of a target business unless and until a sum of money is paid. Unlawful data interception is defined as acquiring, viewing, capturing, or copying non-public data and making it available to someone other than the lawful owner.

These sections within the Cybercrimes Act do not adequately address the complexities of gender-based cybercrimes. Consequently, Sections 7-12 are insufficient in comprehensively dealing with gender-specific cybercrimes. While these provisions encompass offences like hacking, cyber forgery and uttering, cyber extortion, and unlawful data interception, they lack explicit consideration for gender-based cybercrimes. For instance, in cases of sextortion, a distinct form of gender-based cybercrime, the language and scope of these sections are neither inclusive nor sufficient. The provisions, designed to combat unauthorized access, fraud, extortion, and data interception, fall short of capturing the unique dynamics and motives associated with gender-based offences in the digital domain. Therefore, there is a critical need for specialized provisions that explicitly address and penalize gender-based cybercrimes within the legal framework.

[258] S Snail ka Mtuze "The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the cybercrimes act 19 of 2020 and the Protection of Personal Information Act 4 of 2013," (2022) 43(3) *Obiter*.

This section is unclear as to whether it punishes such crimes; one must read it carefully to determine whether the Act covers sextortion. Sextortion, on the other hand, can be defined as "the practice of forcing someone to do something, particularly to perform sexual acts, by threatening to publish naked pictures of them or sexual information about them"[259] This forms part of Gender-based forms of Cybercrime which takes place through sexual exploitation in which the abuse of power is used to coerce, by threatening to release sexual images or information of the victim which have been gained illegally. The described section addresses cybercrimes involving sexual exploitation, specifically those using an abuse of power to coerce victims by threatening to release illegally obtained sexual images or information.

While this provision acknowledges the existence of such crimes, including sextortion, the gap lies in its lack of specificity regarding the types of extortion punishable under the section. To address this gap, Section 10 should be expanded to include all forms of extortion, specifically mentioning sextortion. By specifying and encompassing sextortion explicitly within the legal framework, the section would be more effective in prosecuting and deterring this gender-based cybercrime. The proposed extension would enhance the legal response to sextortion, aligning with the need for precise and inclusive provisions to combat gender-specific cybercrimes comprehensively.

c. Malicious Communication - Sections 7, 8, 9 and 10 of the Act

i. Incitement of threats of damage to property or violence

Malicious communications are addressed in Part II of Chapter 2 of the Cybercrimes Act. This section specifies three different sorts of offences. The Cybercrimes Act criminalises any incitement to violence or threat to cause property damage. It is an offence to release a data message to a person, group of people, or the public via an electronic communications service to encourage the causing and action of property damage or violence against a person or group of people.[260]

It is also illegal to unlawfully and knowingly disclose a data message that threatens a person or group of people with property harm or violence.[261] The provision additionally specifies that

[259] Sextortion (no date) Cambridge Dictionary. Available at: https://dictionary.cambridge.org/dictionary/english/sextortion (Accessed: 26 August 2023).
[260] Section 14 of the Cybercrimes Act.
[261] Section 15 of the Cybercrimes Act.

a reasonable person, possessing the same information, would perceive the data message, whether alone or in conjunction with any other data message or information, as a threat of property damage or violence against a person or group of people. The Cybercrimes Act defines "property damage" as either physical or intangible harm to property.[262] The term 'group of persons' encompasses characteristics that identify an individual as a member of a group, including race, gender, sex, pregnancy, marital status, ethnic or social origin, color, sexual orientation, age, disability, religion, conscience, belief, culture, language, birth, or nationality. Violence is also defined as bodily harm within this context.[263]

The conclusion that Sections 14 and 15 of the Cybercrimes Act exhibit notable insufficienciesin addressing gender-based cybercrimes has been reached by examining the provisions' language, scope, and adaptability. The sections, which primarily focus on threats involving bodily harm or property damage through technology, lack specificity and clarity in addressingthe nuances of gender-based cybercrimes, such as virtual rape and sexual crimes. The broad and vague language in these sections raises uncertainties about their applicability to cases involving virtual rape and sexual intimidation. The conclusion stems from a critical analysis of the text, revealing a gap in the Act's ability to comprehensively address gender-specific cybercrimes, especially those related to sexual offences and virtual violence.

It is important to note that virtual rape is not explicitly defined in the given context, but it typically refers to a form of sexual assault or violation that occurs within virtual environments, such as online spaces or digital platforms. For example, ‘Trolling’ is a new term in the cybersphere considered a form of Gender-based forms of Cybercrime harassment. Trolling can be defined as a deliberate act of luring others into useless circular discussion, with the result of interfering with the positive and valuable exchange of ideas in online discussion sites.[264] While the definition of trolling does not inherently specify a gender-based motive, gender-based cybercrime concerns may arise in scenarios where trolling takes the form of online harassment or abuse, explicitly targeting individuals based on their gender. For instance, if trolling involves the use of sexist language, threats, or the dissemination of explicit content with the intent to harm, intimidate, or humiliate individuals based on their gender, it can be considered a gender-based cybercrime. However, the challenge is that existing legal provisions may not explicitly address the gendered nature of such offences, making it difficult to prosecute trolls under

[262] Cybercrimes Act.
[263] Section 13 of the Cybercrimes Act.
[264] Ibid.

gender-specific cybercrime laws. Moreover, laws may not keep pace with evolving online behaviours, necessitating continuous updates to address and mitigate gender-based cyber threats effectively.

In the context of trolling and online harassment with a gender-based focus, the Cybercrime Act might lack specific provisions to address certain forms of communication that can be classified as gender-based cybercrime. For instance, if the trolling involves explicit and targeted gender-based threats, derogatory language, or the unauthorized sharing of explicit content to harm or humiliate based on gender, it may not be explicitly covered by existing provisions. Incorporating such forms of communication under malicious communications within the Cybercrime Act could enhance legal frameworks to combat gender-based cybercrime. However, the challenge lies in the global nature of these offences, making it imperative for legal systems to evolve and adapt to effectively address the nuanced and evolving dynamics of gender-based cyber threats. The lack of straightforward legal remedies might contribute to a perception among victims that there is insufficient protection against such online harassment.

In the case of *South African National Editors Forum and Others v Black Land First and Others*,[265] the High Court of South Africa issued a broad injunction supporting the media. This injunction barred the respondents from various actions directed towards the applicants, including intimidation, harassment, assaults, threats, home visits, or any behaviour that would violate their liberty. Furthermore, the respondents were prohibited from making threatening or intimidating statements on social media that alluded to violence, harm, or threats.

In South Africa, a family finds themselves in a legal battle against Facebook, the parent company of Instagram, after their teenage daughter received alarming threats via Instagram from an anonymous user.[266] The girl, suspecting the threats originate from someone at her school, fears for her safety and has sought to compel Facebook to disclose the identity of the anonymous account holder responsible for the threats. Despite several unsuccessful attempts,the family has resorted to legal action for resolution.[267] This case highlights the complexities of holding multinational corporations accountable in the digital era

[265] High Court of South Africa in Johannesburg, Case No 23897/17, (2017) (accessible at: http://www.saflii.org/za/cases/ZAGPJHC/2017/179.html).
[266] Daily Maverick, 'Anonymously threatened with gang rape and murder, SA teenager takes Facebook Inc to court to disclose perpetrator' (2020) (accessible at: https://www.dailymaverick.co.za/article/2020-07-24- anonymously-threatened-with-gang-rape-andmurder-sa-teenager-takes-facebook-inc-to-court-to-disclose- perpetrator/).
[267] Ibid.

and prompts discussions on the extent of their obligation to safeguard children using their platforms.

By incorporating provisions within the Cybercrime Act to specifically address gender-based forms of cybercrime, such as trolling with explicit gender-focused threats or derogatory language, the legal system can better adapt to the evolving nature of online offences. Clear and comprehensive provisions would not only empower law enforcement to take effective action against perpetrators but also contribute to a heightened awareness among the public about the legal consequences of engaging in gender-based cyber harassment. This, in turn, can foster trust in the legal system, assuring victims that adequate legal remedies are available to protect them in the digital realm. As technology advances, these provisions would serve as a crucial step in creating a legal framework responsive to the nuanced challenges posed by gender-based cybercrimes, ensuring a safer and more secure online environment for all individuals.

ii. Revenge pornography

Section 16 of the Cybercrimes Act addresses revenge or non-consensual pornography. Revenge pornography, also known as non-consensual pornography or involuntary pornography, involves the distribution of sexually explicit images of an individual, where at least one of the individuals depicted did not consent to the dissemination.[268] Section 16 of the Cybercrimes Act stipulates that "any person ('A') who unlawfully and willfully reveals, through an electronic communications service, a data message containing an intimate photograph of a person ('B') without B's agreement is guilty of an offence."

One criticism directed at the revenge porn provision of the Cybercrimes Act is that criminal consequences are solely directed towards the original perpetrator who initially disseminates the sexually explicit images, with no real repercussions for subsequent sharing by third parties. Snail contends that the Protection of Personal Information Act (POPIA) could potentially address these shortcomings by establishing offenses where the Cybercrimes Act falls short.[269] POPIA sets forth minimum conditions or requirements that must be adhered to when processing personal information. It defines personal information as information pertaining to an identifiable, living, natural person. Notably, a graphic image of a person falls within the purview of personal information. Consequently, legal consequences may ensue for third parties

[268] M Musoni "The Criminalisation of 'Revenge Porn' in South Africa" (2019) *Obiter* 62.
[269] S Snail ka Mtuze, and M Musoni, 'An overview of cybercrime law in South Africa.' (2023) 4 *Int. Cybersecur. Law Rev* 299–323.

who process such images in accordance with the definition for processing outlined in POPIA.

Revenge pornography is when intimate videos or images of a person are placed online without the person's consent.[270] This shared information must have caused the victim harm or anyonein a close relationship with the victim'.[271] However, the Act is silent on the definition of whatis meant by a 'close relationship'. To enhance the effectiveness of the Cybercrime Act in addressing gender-based cybercrimes, it is crucial to consider provisions akin to those in the Domestic Violence Act (DVA) that specifically define and elaborate on the nature of relationships. Like the DVA provision, the Cybercrime Act could stipulate that the shared information causing harm should not only affect the victim directly but also any person "in a close relationship with the victim." However, the current silence within the Act regarding the definition of a 'close relationship' may expose legal frameworks to potential gaps and uncertainties. As relationships continually evolve in the ever-changing landscape of modern society, a clear and inclusive definition of what constitutes a 'close relationship' would provide essential guidance, ensuring that the legal system remains adaptive and robust in addressing the multifaceted dynamics of gender-based cybercrimes.

Early cases in cyberspace, such as *Le Roux v Dey*[272] and *Manyi v Dlamini*[273], paved the way for developing the Cybercrimes Act, which prohibits various cyber offences, including unlawful access. Section 16 of the Act also addresses the unauthorized disclosure of "intimate images." In the *Le Roux v Dey*[274] case, the court affirmed that disseminating intimate images implying a specific relationship status constituted actionable conduct.

Section 16 of the Act focuses on the disclosure of intimate data messages. While Section 16(2)(b)(iii) commendably includes protection for individuals who are transgender or intersex, there is a notable absence of explicit reference to the fact that women and children are often primary targets of online malicious communications. It is crucial to recognize that emphasizing the vulnerability of certain groups, such as women and children, within legislation does not intend to suggest unequal protection but aims to address the reality that these groups are disproportionately affected by cybercrimes like malicious communications. Acknowledging

this in the Act helps raise awareness about the specific challenges women and children face in

[270] Ibid.
[271] Ibid.
[272] *Le Roux v Dey* (2011) 3 SA 274 (CC)
[273] *Manyi v Dhlamini* 2018 ZAGPPHC 563.
[274] *Le Roux v Dey* (2011) 3 SA 274 (CC).

the digital space, fostering a more informed understanding among law enforcement, legal professionals, and the public. It enables a targeted approach to address the unique threats faced by these groups, ultimately contributing to a more effective and inclusive legal framework for combating cybercrime.

In the case *T G v W C (3198/2019) [2020] ZAGPJHC 229*[275] the judge noted, It is crucial to acknowledge that the emergence of social media has significantly amplified the potential for profound and widespread abuse of the dignity of intimate partners. This phenomenon, commonly referred to as 'revenge pornography,' entails the sharing or distribution of nude or sexually explicit material of individuals without their consent and with the explicit intent of humiliating them. Cybercrimes Act and the Films and Publication Amendment Act allows for the victims to pursue criminal charges against anyone who distributes or shares such material on social media platforms, via text messages, through any form of electronic communication, or on pornographic websites. By recognizing the gravity of revenge pornography and affirming victims' rights to seek legal recourse against perpetrators, the judgment underscores the significance of addressing GBV in the digital realm. It also underscores the necessity for legal frameworks that protect individuals from such violations and hold perpetrators accountable for their actions, thus reflecting a growing awareness of the need to address the evolving landscape of cyber-enabled GBV.

According to Musoni, the criterion of consent is crucial as it serves to differentiate between consenting pornography and non-consensual pornography. Musoni argues that in the absence of consent, any processing of intimate data by a third party constitutes a section 16 offence.[276] The Cybercrime Act explicitly outlines the boundaries for viewing intimate images. This provision encompasses both real and simulated images, specifying that it applies when a person's image is depicted unclothed, or when it shows the genital or anal area, or the breast area of a female, transgender, or intersex individual, whether covered or uncovered.[277]

The absence of a provision in Section 16 to address the concerns of victims of revenge pornography from economically disadvantaged backgrounds is a noteworthy gap in the legislation. Including a specific provision to cater to these individuals is essential to ensuringa more inclusive and equitable legal framework. Victims from lower socioeconomic backgrounds may face additional barriers,

[275] *T G v W C* (3198/2019) [2020] ZAGPJHC 229 (28 September 2020).
[276] M Musoni "The Criminalisation of 'Revenge Porn' in South Africa" (2019) Obiter 62.
[277] Section 16 (2) (b) of the Cybercrimes Act.

such as fear of social stigma or discrimination when coming forward with concerns related to revenge pornography. Explicitly acknowledging andaddressing the potential challenges poorer victims face within the legislation would encourage a more open and accessible avenue for reporting and seeking legal recourse. This provision would contribute to a legal system that is sensitive to the diverse circumstances of all individuals, irrespective of their social or economic status, fostering a more just and inclusiveapproach to combating cybercrimes like revenge pornography. Victims may suffer economicloss due to losing their jobs when explicit videos of them emerge.[278]

The Act is silent on this coming from a society whereby putting food on the table for your family will outweigh attending a police station and court to report these incidents, as the desperation of a job will outweigh the fight for justice. Addressing the concerns of victims from economically disadvantaged backgrounds in Section 16 is crucial because the current silence in the Act fails to recognize the socio-economic realities that may deter individuals from reporting revenge pornography incidents. In societies where the daily struggle for survival takes precedence over engaging with law enforcement and the legal system, victims may prioritize securing basic needs like putting food on the table over pursuing justice. Explicitly acknowledging and accommodating the unique challenges poorer victims face within the legislation encourages a more accessible and empathetic approach, recognizing the complex interplay between economic circumstances and seeking legal recourse for cybercrimes.

d. Sentencing

Within the domain of cybercrime, a pivotal aspect of criminal proceedings pertains to the sentencing guidelines delineated in section 19 of the Act, housed within Part V of Chapter 2. Section 19(1) stipulates that contravention of sections 2(1) or (2), 3(3), or 7(2) renders an individual susceptible to a fine or imprisonment for a maximum period of five years, or both.[279] Furthermore, Section 19(2) outlines that individuals who breach the provisions of sections 3(1) or (2), 4(1), 5(1), 6(1), or 7(1) may face a fine, imprisonment for up to ten years, or both. Moving forward, Section 19(3) elucidates that contravening section 11(1) could lead to a fine, imprisonment not exceeding fifteen years, or both.[303]

In addition, Section 19(4) empowers the court to impose a sentence in cases where offenses

[278] Ibid.
[279] S 19(5)(a)–(d) of the Cybercrimes Act.

under sections 8, 9(1) or (2), 10, or 11(2) lack a specified penalty in other laws.[280] The court may apply a sentence as per the provisions of section 276 of the Criminal Procedure Act 51 of 1977, deemed appropriate within its penal jurisdiction. Moreover, Section 19(5) mandates that when issuing a sentence under this section or when convicting someone of electronic theft, certain aggravated factors must be taken into account. These factors, enumerated in section 19(5)(a) – (d), encompass considerations such as the electronic nature of the offense, the extent of harm or loss endured by the victim or others, any financial gains or benefits derived from the offense, and whether the offense was perpetrated in collaboration with others. [281]

Section 19(6)(a) provides that if a person is convicted of any offence provided for in sections 2(1) or (2); 3(1); 5(1); 6(1); 7(1); 8; 9(1) or (2), 10 or 11(1) or (2), if the offence was committed by an individual (or with the cooperation or assistance of another person) who, as a consequence of their responsibilities, functions, or legal authority, was in charge of, in control of, or had access to data, a computer programme, or a computer data storage medium, or a computer system belonging to another person in relation to which the offence was committed.[282]

This is a strict rule imposed on the court by the Act. However, it is trite that there are often exceptions to legal rules.[283] The statutory rule applies strictly, except for instances where substantial and compelling circumstances justify the imposition of another sentence.[284]

Section 19(7) provides that any person who contravenes the provisions of sections 14, 15 or 16 is liable on conviction to a fine or imprisonment for a period not exceeding 3 (three) years orto both a fine and such imprisonment.

The sentencing provisions introduced in the Cybercrime Act are a significant improvement over the provisions of The Electronic Communications and Transactions Act 2002, appear to result from careful consideration, and reflect a proactive approach to combatting all forms of cybercrime.[285] This improvement reflects an admirable dedication to addressing the complexity of cybercrime in a shifting technology ecosystem. The legislation successfully emphasizes the gravity of cybercrime and the necessity for balancing restorative justice and punishment by

[280] Ibid.
[281] Ibid.
[282].
[283] See S v Coetzee [1997] ZACC 2.

[284]S Snail 'The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' 2022 *Obiter Law Journal* 536 .
[285] F Cronje, S Snail, AOlivier, J and Jordaan . *The Cybercrime Act—What you need to know* (2022) 3–4.

introducing a more extensive sentencing criterion.

As the digital world continues to adapt to changing landscapes, the Cybercrime Act's improved sentencing approach signifies a commitment to a legal framework that will effectively address the intricate nature of cybercrimes. Addressing the concerns of victims from economically disadvantaged backgrounds in Section 16 is crucial because the current silence in the Act fails to recognize the socio-economic realities that may deter individuals from reporting revenge pornography incidents. In societies where the daily struggle for survival takes precedence over engaging with law enforcement and the legal system, victims may prioritize securing basic needs like putting food on the table over pursuing justice. By explicitly acknowledging and accommodating the unique challenges faced by poorer victims within the legislation, it encourages a more accessible and empathetic approach, recognizing the complex interplay between economic circumstances and seeking legal recourse for cybercrimes. While there might still be room for further refinement and adaptation specifically to a sub-section dedicated to Gender-based forms of Cybercrime, this development is undoubtedly a positive indication of the legislative system's responsiveness to the dynamics of cyber threats.

d. Protection of complainant from harmful effects of malicious communications

A comprehensive examination of South Africa's response to gender-based cybercrimes reveals notable provisions addressing the protection of complainants from the harmful impacts of malicious communications. In particular, Section 20(1) outlines mechanisms for complainants to seek protective orders from a magistrate's court upon laying charges related to specific offences. These orders can include prohibiting any person from disclosing or further disclosing relevant data messages and compelling electronic communications service providers to removeor restrict access to the implicated data messages. This legal framework signifies an attempt to mitigate the adverse effects of gender-based cybercrimes, forming a critical aspect of South Africa's response to the intersection of cybercrime and GBV. Such an application might seek to prevent any individual from disclosing or further disseminating the data message associated with the accusation or directive of an electronic communications service provider, whose service is utilized to disclose or host the data message connected to the charge, and to eliminate or limit remote access to the data message.[286]

Section 20(2) stipulates that when assessing such an application, the court must take into

[286]S Snail 'The convergence of legislation on cybercrime and data protection in South Africa: A practical approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' 2022 *Obiter Law Journal* 536 .

account any supplementary evidence it considers appropriate, including oral testimony or evidence presented through affidavits, which must be included in the official record of the proceedings. Section 20(3) states that if the court is convinced by prima facie evidence indicating that an offense outlined in sections 14, 15, or 16 has purportedly occurred against the applicant, and if there are indeed reasonable grounds to believe that an individual disclosed the relevant data message, the court may, subject to conditions it deems appropriate.[287]

Section 20 creates a legal remedy to seek interim protective measures during the progression of criminal proceedings. The overarching goal is to safeguard the integrity of data messages associated with the charges and curtail the future dissemination of sensitive content. This approach is integral to the broader topic of South Africa's response to gender-based cybercrimes. Additionally, the provision grants the court authority to direct electronic communications service providers to undertake corrective measures, thereby restricting the spread of potentially harmful data transmissions. This proactive stance aims to uphold the anonymity and integrity of data messages throughout criminal proceedings, acknowledging the role and responsibility of electronic communications service providers in enforcing these protective measures within the context of Gender-based Forms of cybercrime.

There is no universal law that governs cybercrime.[288] Cybercrime 'respects no jurisdiction'; a criminal can be situated in Cape Town and 'perpetuate his act that would have effects in Morocco or anywhere in the world.[289] The fact that this can occur anywhere in the world at any time clearly indicates the importance of international collaboration between countries.

International cooperation is essential to tackle Gender-based forms of cybercrime effectively. According to the Budapest Convention's General Principles of International Cooperation, parties must cooperate as much as possible and by applicable international instruments, uniform or reciprocal legislation, and domestic laws for cybercrime investigations.[290]

The absence of physical borders in Gender-based forms of Cybercrime underscores the necessity for international cooperation and consensus among all nations. It becomes imperative for nations to transcend their interests and join forces to develop comprehensive frameworks that facilitate collective action against Gender-based forms of Cybercrime. Such cooperation

[287] Ibid.
[288] A E.F.G 'Challenges to enforcement of cyber-crimes laws and policy' (2016) 6 (1) *Journal of Internet and Information Systems* 11.
[289] Ibid.
[290] Article 23 of the Budapest Convention.

should be grounded in shared values and a common understanding of the gravity and detrimental impact of these offences. By embracing a collaborative approach, nations can harness their collective resources, expertise, and legal systems to effectively address the multifaceted challenges posed by cybercrime, irrespective of geographical boundaries.

Section 24 of the Cybercrime Act addresses jurisdiction and specifies the offenses that South African courts are empowered to adjudicate. These offenses are delineated in both Part I and Part II of Chapter 2 of the Act. Section 24(1) outlines that any court within the Republic possesses jurisdiction over a cybercrime if the accused individual was apprehended within the territory of South Africa. Additionally, jurisdiction is limited to offenders under Section 24(1)(b), stipulating that the individual to be charged must either be a citizen of South Africa, ordinarily reside in South Africa, or, in the case of a company, be incorporated or registered under any South African law. The common thread underlying the challenge of combating cybercrime lies in the requirement for all its components to originate within the jurisdiction of the Republic of South Africa. This condition presents a significant obstacle given the inherently boundary-less nature of cybercrime, which can propagate its disruptive influence seamlessly across geographical boundaries, affecting any technologically connected location worldwide.

Section 24(2) echoes similarly to section 24(1); however, if the listed offences occur outside the Republic's jurisdiction and if the person is not a person contemplated in section 24(1), then the offence can be deemed to be committed in the Republic if '(a) that person is extradited tothe Republic; or (b) that person is found to be in the Republic even if they are not extradited inthe Republic.'

This appears to be a valuable tool to tackle Gender-based forms of Cybercrime that occur in the Republic even if the offender is a foreigner to the Republic. However, to 'apprehend many of the more dangerous criminals, international cooperation is vital'.[291] Gender-based cybercrimes are on the rise, albeit without receiving the necessary attention in the cyberworld. However, if not addressed with targeted care and embedded solutions, there is a risk of compromising security systems and creating potential vulnerabilities. Presently, gender-based cybercrimes are perceived as a comparatively lesser threat on the international stage, akin to challenges posed by issues like money laundering and trafficking in women for the international sex trade.[292] The irony is that cyber criminals can use technological advancements

[291] A E.F.G , 'Challenges to enforcement of cyber-crimes laws and policy' (2016) 6 (1) *Journal of Internet and Information Systems* 11.
[292] Ibid.

to increase sex trafficking and other crimes that would ordinarily need to be physically committed; thus, it will invertedly be a frontier for gender-based cybercrime globally.

Section 24 (4) states that a prosecution of a listed offence committed outside the Republic '(i) may only be instituted against a person with the written permission of the National Director of Public Prosecutions'. The seriousness of the crime is not taken into consideration here. Awaiting written permission from the National Director of Public Prosecutions will be time constraining. This provision creates a barrier to justice for victims of gender-based cybercrimes, particularly those involving personal and sensitive aspects like the release of intimate images or threats for financial gain. The associated time delays contribute to helplessness and a diminished sense of dignity among victims. Technology is used to facilitate violence, abuse, and harassment against women, including human rights defenders, women inpolitics, and journalists.

This alarming statistic requires solid and unified international cooperation to remedy. The Cybercrime Act, however, is silent and does not include any specific provisions for international cooperation presently. However, in the future, this will become a vital component in gender-based forms of cybercrime cases. The Cybercrimes Act should incorporate provisions for robust national and international cooperation, fostering a culture of seamless collaboration within the global cyber community. This includes mechanisms to streamline information sharing, coordinate investigations, and facilitate swift response to cyber threats across borders, ultimately enhancing the collective cybersecurity efforts nationally and internationally.

e. Additional provisions in the Cybercrimes Act

i. Powers to investigate, search, access or seize

Specific regulations of the Cybercrimes Act,[293] including most of Chapter 4, took effect on December 1, 2021.[294] In addition to creating cybercrime-related offences,[295] the Cybercrimes Act regulates the powers of the police and investigators to investigate cybercrimes. Chapter 4 of the Act underlines the power of the police and other parties regarding search, access, and seizure powers.[296] The provisions of the Criminal Procedure Act apply to the investigation of cybercrimes. They operate in addition to the provisions of Chapter 4 of the Cybercrimes Act to the extent that the Criminal Procedure Act is not inconsistent with the Cybercrimes Act.

[293] Cybercrimes Act 19 of 2020.
[294] Proc R 42 in GG No 45562 of 2021-11-30
[295] Ch 2 of the Cybercrimes Act
[296] In terms of s 28 of the Cybercrimes Act, a police official may, in accordance with Ch 4 of the Cybercrimes Act, search for, access or seize any article, within the Republic.

The Cybercrimes Act grants magistrates and High Court judges the authority to sign search and seizure warrants.[297] In contrast to the Criminal Procedure Act, justices of the peace do not possess such authority under the Cybercrimes Act. Trial warrants may only be issued by "a magistrate or a judge of the High Court presiding over criminal proceedings" according to the Cybercrimes Act. This provision differs from the Criminal Procedure Act, which mentions a judge or a presiding officer in criminal proceedings.

The significance of incorporating provisions for practical national and international cooperation within the Cybercrimes Act becomes evident when considering its implications for law enforcement and cross-border cyber investigations. Unlike the Criminal Procedure Act, which explicitly references judges or presiding officers in criminal proceedings, the Cybercrimes Act lacks clarity regarding the involvement of regional magistrates in issuing search and seizure warrants, both pre-trial and during trial stages. This ambiguity raises concerns about the potential exclusions of regional magistrates and judges from this process. Establishing provisions for seamless collaboration at the national and international levels is essential for addressing the global nature of cybercrimes and ensuring a unified and effective response, avoiding jurisdictional gaps, and upholding the principles of justice in the cyber realm.

The Cybercrimes Act must be interpreted so that regional magistrates can issue both types of warrants.[298] This is because, unlike the Criminal Procedure Act, the Cybercrimes Act neither defines nor expressly excludes regional magistrates from the definition of "magistrate." The Magistrates Act,[299] states that the rules that dictate how magistrates are chosen and how long they serve. The Act define a magistrate as someone appointed according to specific sections of the Magistrates' Courts Act and the Magistrates Act. This excludes individuals serving in an interim or temporary capacity, as well as acting magistrates.[300] The Magistrates Act, outlining the appointment and terms of service for magistrates, plays a significant role in the broader topic of gender-based cybercrimes. Understanding the definition of a magistrate according to this Act is crucial for analyzing the legal landscape related to cybercrimes with a gender-based focus. This definition clarifies the status and authority of judicial officers in handling cases related to gender-based cybercrimes, shaping the framework within which legal proceedings

[297] S 29(1)(a) of the Cybercrimes Act.

[298] PG Du Toit, (2023) "The search warrant provisions of the cybercrimes act and their relationship with the Criminal Procedure Act," (2023) 43(4) *Obiter*.
[299] Act 90 of 1993
[300] S 1 of Act 90 of 1993

are conducted. Section 9 of the Magistrates' Courts Act[301] addressesthe appointment of district and regional court magistrates.[302] It would be illogical if the legislature authorised district court magistrates and High Court judges to issue search warrants (especially when presiding over a criminal trial) but excluded regional magistrates, who should be equally competent and skilled in assessing the authorization of search warrants.[303]

The Cybercrimes Act strongly focuses on addressing cybercrime and incorporates provisions that account for technological advancements, resulting in a more precise description of the items that can be seized under its provisions. The term "article" refers to any data,[304] computer programme,[305] computer data storage medium,[306] or computer system[307] in this context. Each of these articles is defined further in the provisions pertaining to definitions.[308] The significance of the Magistrates Act, especially in defining the term "magistrate," is particularly relevant in the context of gender-based cybercrimes for several reasons. Magistrates play a pivotal role inthe legal process, including issuing orders and warrants that may be crucial in investigating and prosecuting cybercrimes. Understanding the definition and scope of magistrates under this Actis vital for comprehending the legal framework surrounding gender-based cybercrimes and the role that judicial officers, like magistrates, play in addressing these offences. The definition's connection with gender-based cybercrimes is that magistrates, as defined by the Magistrates Act, have the authority to issue orders related to the investigation and evidence-collection process. This understanding is fundamental for ensuring that legal procedures are followed appropriately in cases involving gender-based cybercrimes, reinforcing the significance of the Magistrates Act within the broader topic.

According to the Cybercrimes Act's definition of "article," offences are specifically delineated to include those falling under Part I and Part II of Chapter 2, any other offence within the laws of the Republic, or offences in foreign states that closely resemble those outlined in Part I or Part II of Chapter 2 or are otherwise recognized within the Republic. This broad definition ensures that cybercrimes are comprehensively addressed, encompassing domestic and international legal frameworks. Incorporating offences from foreign jurisdictions that align with those identified in the Act enhances the Act's effectiveness in combating cybercrimes with a global

[301] Act 32 of 1944
[302] S 9(1)(a) of 32 of 1944.
[303]. PG Du Toit, (2023) "The search warrant provisions of the cybercrimes act and their relationship with the Criminal Procedure Act," (2023) 43(4) *Obiter*.
[304] S 1(1)(a) of the Cybercrimes Act.
[305] S 1(1)(b) of the Cybercrimes Act.
[306] S 1(1)(c) of the Cybercrimes Act.
[307] S 1(1)(d) of the Cybercrimes Act.
[308] S 1(1) of the Cybercrimes Act.

perspective, fostering cooperation and alignment with international efforts to addresscyber threats.[309]

Seizable items are not limited to those that are in some way associated with the commission of Cybercrimes Act-created offences. The search and seizure operation may pertain to any crime where data, a computer programme, a computer data storage medium, or a computer system is involved in the commission of the crime or may provide evidence of its commission. This is an essential tool as Gender forms of Cybercrimes can be shared through computer programmes and stored on additional hard – drives involved with the crime's commission. The significance of the expanded scope of seizable items, as outlined in the Cybercrimes Act, lies in its broad applicability to a wide range of crimes involving data, computer Programmes, storage mediums, or computer systems. This extension goes beyond offences explicitly created by the Cybercrimes Act, allowing search and seizure operations to cover any crime where these elements play a role in committing the offence or may serve as evidence. This flexibility is crucial as it provides authorities with a comprehensive legal basis for investigating and gathering evidence in the context of Cybercrimes Act-created offences and a broader spectrum of criminal activities involving digital elements. This means that seizure operations may continue for items which have been used and shared with other devices as evidence for the commission of the crime. It will remain important that the items to be seized are identified with sufficient specificity in both the application for the warrant and the search warrant itself.[310]

In terms of the Cybercrimes Act, the application must prove that the article (i) is within the magistrate's or judge's area of jurisdiction,[311] or (ii) is being used or involved in or has been used or involved in the commission of an offence and there are reasonable grounds to believe that the article is within the area of said jurisdiction.[312]

Cybercrimes and computer-related offenses often present challenges in determining their exact location. As a result, if it seems to the issuing authority that the item in question is within the Republic but its specific jurisdiction is unclear in relation to the offense, a warrant may still be authorized.[313] The flexibility in issuing warrants without precise jurisdictional information, as stipulated in the context of gender-based cybercrimes, is a double-edged sword. While it addresses the urgency of these offences, it also poses potential weaknesses, especially

[309] Ibid.

[310] *Minister for Safety and Security v Van der Merwe.*
[311] S 29(1)(a)(i) of the Cybercrimes Act.
[312] S 29(1)(a)(ii)(aa) of the Cybercrimes Act.
[313] S 29(1)(a)(ii)(bb) of the Cybercrimes Act.

regarding protecting individuals' rights. In the realm of gender-based cybercrimes, time is a critical factor due to the rapid dissemination of evidence and sensitive information. The expedited process of issuing warrants without precise jurisdictional information is justified by the urgency of search, seizure, and confiscation, aligning to protect victims' dignity. However, the potential weakness arises in balancing swift action and ensuring that individuals' rights, including privacy and due process, are adequately safeguarded. Therefore, the specific issue for gender-based cybercrimes lies in managing this trade-off effectively to both address the immediacy of these offences and uphold the rights and dignity of the victims. The nature of computer crimes makes it difficult to pinpoint the precise location, and the lost time will be detrimental to the protection of the dignity of the victim.

These jurisdictional details must be presented to the judicial officer evaluating the warrant. A judicial officer issuing a warrant must ensure that the affidavit offers sufficient evidence of the presence of jurisdictional facts. If not, the judicial officer must refuse to issue the warrant. [314] This requirement serves as a safeguard to strike a balance between the urgency of responding to gender-based cybercrimes and protecting individuals' rights, reinforcing the importance of a judicious and evidence-based approach in obtaining warrants for search, seizure, and confiscation processes. In accordance with the Justices of the Peace and Commissioners of Oaths Act,[315] the affidavit supporting the application for a search warrant must be properly signed before it can be presented to the commissioner of oaths. If the affidavit were drafted and signed before its presentation to the commissioner of oaths for the administration of the oath, the warrant issued on this basis would be null and void.[316]

The Criminal Procedure Act[317] and the Cybercrimes Act[318] permit warrantless searches under exigent circumstances or when consent is granted. The Cybercrimes Act offers a special interim process: an oral request for a warrant (or a warrant modification) in cases of urgency or other exceptional situations. This applies when it is not feasible to submit a written application due to the urgency of the situation or the presence of extraordinary circumstances[319] a specifically designated police official may make an oral application".[320] The application must also comply with any additional directives regarding oral applications that the Chief Justice may issue

[314] *Minister of Safety and Security v Van der Merwe.*
[315] Act 16 of 1963.
[316] *Mogale v Minister of Safety and Security* 2016 (2) SACR 682 (GP). Also see *S v Malherbe* 2020 (1) SACR 227 (SCA).
[317] S 22 of the Criminal Procedure Act
[318] S 32 of the Cybercrimes Act.
[319] S 30(2)(a) of the Cybercrimes Ac
[320] S 30(1) of the Cybercrimes Act.

pursuant to the Superior Courts Act.[321] The Act specifies the prerequisites for issuing a warrant based on an oral application.[322] In addition to the standard requirements for the granting of a warrant,[323] it must be evident that the warrant is immediately necessary to search for, access, or seize an article[324] and that it is not reasonably practicable, giving regard to the urgency of the case or the existence of exceptional circumstances, to make a written application for the issuance of a warrant or to amend an existing warrant.[325] Gender-based forms of Cybercrime constitute unknown territory and are completely unpredictable as technology is constantly evolving. The warrantless search and oral application are a step in the right direction to protect investigators from unknown territory and not impede the development of the investigation.

The Cybercrimes Act introduces a distinctive interim procedure allowing for oral applications for warrants, particularly in cases of urgency or exceptional circumstances. This provision enhances the responsiveness to urgent situations related to gender-based cybercrimes, strengthening the case against GBV. However, it is essential to note that while the Act outlines prerequisites for issuing a warrant based on an oral application, there is a potential vulnerability in the absence of specific considerations related to the unique challenges and sensitivities of gender-based cybercrimes. The Act could benefit from explicit directives addressing the distinctive nature of such offences to ensure a robust and victim-centric approach in oral warrant applications.

According to the Cybercrimes Act, a search warrant mandates the specified officer to search, access, or seize the identified item.[326] This includes the authority to search individuals mentioned in the warrant enter and search designated premises, containers, vehicles, facilities, ships, or aircraft. It is noteworthy that even if there is a technical error in the address, the warrant remains valid if the premises are adequately described. The warrant also empowers the search of individuals believed to possess information relevant to the investigation, especially those near the identified locations or in control of relevant data and systems. This provision is crucial in addressing gender-based cybercrimes, allowing for the targeted search and seizure of articles pertinent to these offences and obtaining necessary tools or information deemed essential for the investigation.[327]

[321] 10 of 2013. See s 30(2)(b) of the Cybercrimes Act.
[322] S 30(4) of the Cybercrimes Act
[323] S 30(4)(a)(i) of the Cybercrimes Act
[324] S 30(4)(a)(ii) of the Cybercrimes Act.
[325] S 30(4)(a)(iii) of the Cybercrimes Act.
[326] S 20(2)(h) of the Cybercrimes Act.
[327] Ibid.

It should be mentioned that the Act imposes specific limitations on using the instrument, device, password, decryption key, or information to gain access to the article mentioned in the warrant.[328] The limitations placed on using specialized tools, as mentioned in the Cybercrimes Act, are crucial to ensure their lawful and ethical deployment. These restrictions are designedto guarantee that tools and information are utilized within the confines of the law and for the specific authorized purposes for which they were obtained. This ensures law enforcement agencies adhere to legal and ethical standards while employing technology to combat gender-based cybercrimes. These limitations within the Cybercrimes Act, governing the use of tools and information obtained through search warrants, are integral to ensuring lawful and authorized usage. The Act's validity requirements, outlined for search warrants, align with common law intelligibility standards established by the Constitutional Court in *Minister of Safety and Security v. Van der Merwe*.[329] These standards include addressing a named police official, identifying the searcher, specifying conferred authority, detailing the person or premises to be searched, precisely describing the article, and specifying the offence triggering the investigation. The linkage between these validity requirements and common law intelligibility is crucial, as any material errors in describing the offence may render the searchand seizure warrant invalid, emphasizing the importance of precision and clarity in the legal framework. This connection is significant in the context of gender-based cybercrimes, ensuring that the legal procedures uphold the rights of individuals and adhere to established standards.[330]

There has been academic and judicial contention of whether separate judicial authorization is required for the seizure of computer or device hardware, on the one hand, and accessing and retrieving data from the device, on the other, has been the subject of scholarly and judicial discussion. Bouwer believes that each step requires judicial authorization. [331] In *S v Miller*,[332] judge Gamble J found that such an approach is unnecessary after analysing the relevant provisions of the Electronic Communications and Transactions Act and their relation to the Criminal Procedure Act.

[328] S 37(2)(a) of the Cybercrimes Act.

[329] When a statutory offence is being investigated, the search warrant should reference the precise statute and the relevant section or subsection. This is important so that both the person in charge of the premises to be searched and the law enforcement officer authorised to execute the search warrant are aware of the offences for which the search has been authorised.

[330] *Oosthuizen v Magistrate, Hermanus* 2021 (1) SACR 278 (WCC) 59.

[331] GP Bouwer 'Search and seizure of electronic evidence : division of the traditional one-step process into a new two-step process in a South African context' (2014) 27 (2) *South African Journal of Criminal Justice* 156–71.

[332] 2016 (1) SACR 251 (WCC).

In *Oosthuizen v the Magistrate*[333], Hermanus, Norton AJ emphasized the necessity for a warrant to meet certain requirements. Firstly, it must clearly state that the purpose of the search, particularly concerning electronic devices, is to locate material stored on them. Secondly, the warrant must identify the relevant material by linking it to the suspected offenses, and it should reference the types of electronically stored data, such as accounting records, invoices, correspondence, photographs, or videos, that could potentially serve as evidence for those offenses. This level of detail is crucial to enable the searching police officers to distinguish between electronically stored material that can be seized and material that cannot.[334]

An examination of the Cybercrimes Act reveals that distinct authorizations are required to seize equipment and access data. Even the method used to obtain access to data itself must be authorised. However, the authorization for these many operations may be contained in a single search and seizure warrant.

On the other hand, the Cybercrimes Act permits the execution of a search order at any time unless the person granting the request indicates otherwise in writing.[335] Regarding Gender-Based forms of Cybercrime, electronic evidence, including social media accounts, online chat profiles, cell phones, explicit pornographic material videos, and sex chat rooms, can be quickly deleted or destroyed. Hence, it is crucial that search warrants can be executed both during the day and night, but with careful consideration. Authorization for night-time searches should not be granted carelessly, particularly when it involves searching individuals and property. This is because such searches during night-time may pose heightened risks to the safety and well-being of law enforcement officers and individuals at the location. The reduced visibility and potential for increased tension during night-time operations necessitate a cautious approach to protect all parties involved and prevent unintended consequences or misunderstandings that may arise in low-light conditions.

Providing a copy of the warrant upon execution is not considered prior notice. The intent is to prevent potential dangers wherein individuals whose rights are affected by a search and seizure operation might delete or destroy evidence if given advance notice. The provision aims to secure the investigation's integrity and preserve crucial evidence by minimizing the likelihood of tampering or destruction when individuals become aware of the impending operation.[336]

---

[333] *Oosthuizen v Magistrate, Hermanus* 2021 (1) SACR 278 (WCC) 59.
[334] *Oosthuizen v Magistrate, Hermanus* 2021 (1) SACR 278 (WCC) 59. For a more detailed discussion of the case see Du Toit 2021 2 South African Journal of Criminal Justice.

[335] S 29(4)(a) of the Cybercrimes Act.
[336] *Thint (Pty) Ltd v NDPP, Zuma v NDPP* 2008 (2) SACR 421 (CC) 98.

Under the Criminal Procedure Act, if a search warrant is being executed by a police officer, they are required to furnish a copy of the warrant to any individual whose rights were infringed upon by the search, if requested.[337] The Supreme Court of Appeal has decreed that, along with the search and seizure warrant, the affidavit supporting the application for the warrant must also be included and provided to any individual affected by the search upon request. This ruling aims to expedite any court proceedings that may arise if a person claims that their Constitutional rights were violated during the search.[338] Ally raises two objections to this provision. First, he believes that a copy of the warrant should be presented whenever possible before the search and seizure. Second, the delivery of a copy should not rely on the individual's request, as many subjects will not make such a request due to their lack of legal knowledge.[339]

The Cybercrimes Act addresses these concerns by mandating that the police officer executing a search warrant must provide a copy of both the warrant and the officer's written application to any individual whose rights have been affected in relation to any search or item accessed or seized under the authority of the warrant.[340] The transfer of the warrant and its application isn't contingent on the request of the individual whose rights are infringed upon by the search. These requirements ensure that both the warrant and its application are handed over. This implies that the affidavit or sworn declaration supporting the application must be provided as well.

Additionally, a search warrant issued under the Cybercrimes Act may authorize an investigator or another designated individual to assist the police officer specified in the warrant by providing technical support for the search, access, or seizure of the item in question, as specified in the warrant.[341] The violation of this provision constitutes an offence.[342] Acontravention of Section 35 is to obstruct or hinder a police officer using his or her authority under sections 28 and 29 of the Act.[343] Police officials are empowered to use force.[344]

The provisions of the Criminal Procedure Act were frequently utilized to search for and confiscate items now included under the Cybercrimes Act. The criticism centres on the notion that the search and seizure provisions of the Criminal Procedure Act have not effectively adapted to technological advancements.[345] Therefore, introducing investigation instruments in the

[337] S 21(4) of the Criminal Procedure Act.
[338] *Goqwana v Minister of Safety and Security*
[339] Ally in Joubert (ed) *Criminal Procedure Handbook* 196.
[340] S 29(5) of the Cybercrimes Act
[341] S 29(5) of the Cybercrimes Act
[342] S 29(3) of the Cybercrimes Act.
[343] S 34(2) of the Cybercrimes Act.
[344] S 35(1) of the Cybercrimes Act.
[345] S 35(2) of the Cybercrimes Act.

Cybercrimes Act is crucial, providing an opportunity to address emerging forms of crimesand enhance search and seizure provisions. Specifically, this includes addressing gender-based forms of cybercrime, necessitating developing and improving search and seizure mechanismswithin the legal framework. Strict adherence to the requirements outlined in the Act for searchwarrants is essential, but it's also important for issuing officials to comply with additional requirements established by our superior courts. This ensures the validity of warrants, which may be challenged during preliminary litigation or at trial, particularly regarding the admissibility of evidence obtained through a search warrant. To prevent the issuance of multiple search warrants for a single criminal investigation, the search and seizure provisions of the Cybercrimes Act should be incorporated into the Criminal Procedure Act.[346]

ii. Mutual Assistance

In accordance with Section 46 of the Act, Sections 48 to 51 apply in addition to the International Cooperation in Criminal Matters Act.[347] Section 47 allows the National Commissioner or National Director to share information with a foreign law enforcement agency.[372] Section 48 pertains to requests for aid and cooperation from foreign governments. It stipulates that a designated point of contact may legally forward requests for information to a foreign authority, court, or tribunal.[373]

Section 49 stipulates that an electronic communications service provider or financial institution must comply with an order issued by a designated judge pursuant to section 48(6). [374] The National Director of Public Prosecutions (NDPP) is required by Section 50 to advise the designated court or applicable authority in a foreign state of the outcome of a request for help and collaboration.[375] Section 51 enables issuing an order seeking cooperation from a foreign state.[376]

This significant development represents a positive step forward, particularly in addressing crimes related to Gender-based Cybercrime. Given that these offences frequently occur on social media platforms as a means of execution, it is critical to recognise that many social media companies operate as foreign entities. This involves collaborating with national agencies to improve access to information through communication and relationships with these corporations' central headquarters. This method recognises the complexities involved and is a practical step forward in efficiently dealing with cross-border Gender-based Cybercrime.

[346] PG Du Toit, (2023) "The search warrant provisions of the cybercrimes act and their relationship with the Criminal Procedure Act," (2023) 43(4) *Obiter*.
[347] Act 75 of 1996.

iii. Evidence

Section 53 allows for the use of affidavits to present evidence related to various aspects of technology and computing, including the interpretation of data, the design or operation of S 47(1) of the Cybercrimes Act. S 48(1) of the Cybercrimes Act. S 49(1) of the Cybercrimes Act. S 50(1) of the Cybercrimes Act. S 51(1) of the Cybercrimes Act computer Programmes, data storage mediums, computer systems, electronic communication networks and technology, software engineering, and computer programming. This clause makes expertise a requirement for such evidence[348] and creates an offence to produce misleading and false information as evidence.[349]

Digital evidence can be altered or erased quickly, creating difficulty in establishing cybercriminals' guilt.[350] Chapter 7 of the Cybercrimes Act deals with evidence, and S53 herein requires proof of specific facts to be produced on affidavit. Section 53(4) clarifies that the provisions of Section 53 do not impact any other existing laws that allow for the admissibility of certificates or other documents as evidence. Additionally, it specifies that the provisions of Section 53 are to be considered as supplementary to, rather than a replacement for, any such existing laws.

Chapter 7 should incorporate provisions addressing the unique nature of evidence in the context of Gender-Based forms of Cybercrimes. These online attacks and threats have the potential to be easily erased, with the perpetrator's identity often unknown. The standard of evidence for Gender-Based forms of Cybercrimes should balance the victim's sensitivity and the stringent evidential requirements, facilitating victims' willingness to come forward without the fear of falling short of strict evidential criteria. Enhancing the Cybercrime Act's approach to evidence collection could involve implementing educational initiatives for police officers to ensure a comprehensive understanding of handling electronic evidence.

i. Reporting obligations and capacity building

The Cybercrimes Act's Sections 54 to 57 are contained in Chapter 8. Section 54 mandates that a provider of electronic communications services must notify the SAPS within 72 hours of becoming aware of a violation of Part I of Chapter 2.[351] It is crucial to highlight that non-

[348] S 53(1) of the Cybercrimes Act.
[349] S 53(2) of the Cybercrimes Act.
[350] at12; x
[351] S 54(1) of the Cybercrimes Act.

compliance with this provision constitutes an offence, subject to a fine not exceeding R50,000.[352]

This provision is deficient due to its absence of explicit procedural guidelines and a lack of specificity regarding the types of electronic communications service providers it encompasses. Additionally, there is a notable absence of clarity on the protection and incentives afforded tothese service providers, raising concerns about potential repercussions for internal whistleblowers within the organization. The Act establishes a provision for imposing fines without incorporating formal accountability mechanisms to monitor the future operations of electronic communications service providers. This lack of accountability mechanisms raises concerns about the potential misuse or inadequate regulation of electronic communications service providers in the context of gender-based cybercrime. Specifically, without proper monitoring, there may be a risk of these providers not adequately addressing or preventing gender-based cybercrimes, potentially leaving victims without sufficient protection.

Section 55 mandates that the cabinet minister overseeing policing must establish and sustain adequate human and operational resources to detect, prevent, and investigate cybercrimes.[353] It also ensures that police officials have the necessary training[354] and develop accredited training programmes for SAPS members in cooperation with higher education institutions.[355] While the initiative to develop a curriculum and training Programmes for the SAPS is a positive step, it is noteworthy that there is currently no explicit inclusion of Gender-Based forms of Cybercrime in these efforts. To enhance the effectiveness of law enforcement in addressing the complexities of cybercrimes with a gender-specific focus, it is advisable to explicitly state that the curriculum and training Programmes should encompass gender-based cybercrimes. This would ensure that officers are adequately equipped to handle and respond to gender-based incidents within the cybercrime landscape. The inclusion of Gender-based forms of Cybercrime training in these programmes will help magnify the existence of this in the worldof cybercrime and equip our police officers with the necessary skills and tools to engage withvictims of Gender-based forms of Cybercrime appropriately.

Section 56 of the Act, which mandates the NDPP to maintain statistics on cybercrime prosecutions,[356] may be well-intentioned, but its efficacy is questionable. The real challenge

[352] S 54(3) of the Cybercrimes Act.
[353] S 55(1)(a) of the Cybercrimes Act.
[354] S 55(1)(b) of the Cybercrimes Act.
[355] S 55(1)(c) of the Cybercrimes Act.
[356] S 56(1) and (2) of the Cybercrimes Act.

lies in the insufficient emphasis, training, and knowledge provided within police stations, particularly considering the hurdles faced by complaints related to Gender-Based forms of Cybercrime during the prosecutor docket pool stage. Instead of solely focusing on statistics for prosecutions, there is a critical need for comprehensive capacity building within law enforcement to enhance the investigation of cybercrimes, including gender-based incidents. Additionally, the NPA should provide detailed statistics that are disaggregated to reflect the nature of cybercrimes, aiding in tracking incidence and prosecution rates, particularly for gender-based cybercrimes.

The provision should have emphasized that "The NDPP maintains statistics on cybercrime reporting and challenges from complaint to conviction." It is crucial to recognize the distinction between the responsibilities of SAPS, which reports crime statistics, and the NDPP, which reports prosecution and conviction statistics. Section 55 aptly highlights the disconnect between the challenges individuals face on the ground and the difficulties encountered in registering complaints for Gender-Based forms of Cybercrime.

Section 57 of the Cybercrimes Act gives the National Executive the authority to enter into agreements with foreign states, particularly concerning offences under Part I or Part II of Chapter 2. This provision, especially under S1(a)(i), proves beneficial for overcoming budget constraints and resource limitations, enhancing South Africa's capabilities to address crimes when facing inadequacies in tools and resource capacity. Additionally, S1(a)(iii) includes offences similar to those contemplated in Part I or Part II of Chapter 2, encompassing Gender-Based forms of Cybercrime. While commendable, the exponential growth of Gender-Based forms of Cybercrime might warrant a dedicated section. Moreover, S1(b) emphasizes the importance of implementing cybercrime response activities, including training, research, information and technology-sharing, and exchanging information on the detection, prevention, mitigation, and investigation of cybercrimes. This provision is instrumental in shaping the necessary skill set and reactive measures crucial for swiftly combatting Gender-Based forms of Cybercrime.

Gender-based forms of cybercrime, in themselves, are facets of the broader issue of GBV and discrimination. The internet age has provided fast access to information and has, unfortunately, also paved the way for the evolution of GBV.[357] 'The internet is also becoming a place of choice for traffickers to sell sexual services they force upon their

[357] LM Rhodes 'Human trafficking as cybercrime' (2012) *AGORA International Journal of Administration Sciences*

victims'.[358] The pressing challenge posed by Gender-Based Forms of Cybercrime underscores the imperative for law enforcement agencies, including those in South Africa, to possess adequate resources and funding. As cybercriminals demonstrate agility and sophistication in their activities, empowering law enforcement with essential tools and capabilities becomes crucial. Section 57 of the Cybercrimes Act is pivotal in facilitating necessary interventions by allowing the National Executive to enter into agreements with foreign states when addressing offences outlined in Chapter 2. This provision is critical to strengthening law enforcement's capacity tocombat cybercrimes effectively. Technological tools exist to fight cybercrime on the surface and the dark web'.[359] Developing specialized tools to address the unique challenges posed bygender-based cybercrime is essential. An exemplary tool is "Spotlight," which was created through a collaboration between Thorn and Digital Reasoning.[360] This tool is designed to remove publicly available information from the internet, analyze it, and assist law enforcement in prioritizing cases related to child trafficking. By concentrating data and expediting the police response time, Spotlight illustrates the potential for specialized tools to enhance the effectiveness of law enforcement in combating specific forms of cybercrime. Similar tailoredtools could be developed to address the nuances of gender-based cybercrime, offering law enforcement the necessary means to navigate and combat these offences more efficiently.[361]

For example, Spotlight is a tool created by Thorn in partnership with Digital Reasoning. This removes publicly available information from the internet, analyses it, and uses it to help prioritize law enforcement cases.[362]The focus of this programme is to combat child trafficking data and speed up the police response time by facilitating 'concentrated data to work with'.[363]

Technological tools are being developed to combat Gender-based forms of Cybercrime. However, a joint effort is required globally to make it fully operational in a manner that considers the circumstances of both developed and developing nations.

[358] Ibid.
[359]LM Rhodes 'Human trafficking as cybercrime' (2012) *AGORA International Journal of Administration Sciences*
[360] Ibid.
[361] Ibid.
[362] Ibid.
[363] Ibid.

III. ABILITY OF CYBER CRIMES ACT TO GIVE EFFECT TO NSP ON GBV

a. South African Government National Strategic Plan

South Africa has devised a National Strategic Plan (NSP) spanning from 2020 to 2030 to combat GBV and Femicide (GBVF), in response to the crisis highlighted during the Presidential Summit of 2018. This comprehensive plan seeks to offer a coordinated and cohesive strategy, policy, and programming framework across various sectors to bolster the government's and the nation's collective response to Gender-Based forms of Cybercrime. Oneof its key focuses is tackling online violence, with a recognition of the heightened vulnerability faced by young women, who often experience a disproportionate level of such abuse in digital spaces.[364] The NSP urges technology intermediaries to adhere to human rights standards in safeguarding women's rights on online platforms and in new technologies. It advocates for the development and implementation of cyber-violence and cyber-awareness programmes that are accessible to people with disabilities, along with efforts to promote online safety. Additionally, it calls for the enhancement of the capacity of law enforcement, prosecutors, and the judiciary to effectively address emerging cyber threats, particularly those related to gender-based cybercrimes. The NSP emphasizes the urgent implementation of legislative measures to address deficiencies in managing gender-based cybercrime cases. Furthermore, it underscores the importance of conducting research to better understand the impact of online violence on women and LGBTIQ individuals, as well as to identify potential solutions.[365] Even though isolated frameworks providing legal protections exist in different sectors/cases, the research shows that no specific legislation focuses solely on Gender-based forms of Cybercrime. Due to a lack of specific legislation and policies, many women, girls, and LGBTIQ people are at risk of being disproportionately affected by gender-based cybercrimes.However, there are opportunities in existing legislation to strengthen the law and include OGBV provisions. The Domestic Violence Amendment Bill of 2020, for example, could potentially provide some forms of protection in the context of Gender-based forms of Cybercrime such as cyber harassment, cyberstalking, and non-consensual image sharing.[366]

---

[364] UN Women "The views expressed in this publication are those of the authors and do not necessarily represent the views of UN Women, the United Nations or any of its affiliated organizations." (2019) Safe Digital Spaces: Protection of Women and Girls from Technological Violence http://africa.unwomen.org/en/digital-library/publications accessed on 4 March 2023.
[365] Ibid.
[366] Ibid.

In South Africa, women and LGBTIQ people are frequently subjected to online harassment. Although data are scarce on the extent and prevalence of Gender-based forms of Cybercrime in the physical world compared to GBV, the available information suggests that it has the potential to spiral out of control if not addressed seriously. According to gender-based cybercrimes are primarily occurring in South Africa via social media platforms such as Facebook, WhatsApp, and Twitter, with varying consequences for individuals. For example, Gender-based forms of Cybercrime against female journalists are an increasingly dangerous form of media silencing that endangers not only their safety and well-being but also the diversity of voices in the media, as well as freedom of expression and access to information. People who have experienced gender-based cybercrimes use various coping mechanisms, such as reporting the phenomenon, deleting, blocking, or completely withdrawing from the platforms. To end Gender-based forms of Cybercrime, various stakeholders must work together, and the international instruments must be effective in this regard.[367]

The emergence of Gender Based forms of cybercrime has presented substantial reporting and enforcement challenges for law enforcement organisations and judicial systems worldwide.[368] Often, individuals represent the weakest link in computer security, as their vulnerabilities can be exploited in different ways depending on the type of cybercrime. This can result in victims unwittingly becoming instruments of their own victimization. Methods of exploitation include sexual exploitation, deception, manipulation of decision-making processes through perceived urgency or authority, and the use of predictable patterns such as website usage, downloads, password habits, and social or professional networking to access victims' private data.[369]

In addition to potentially devastating consequences such as financial loss or harm to reputation and professional careers, victims may also experience self-blame or be held accountable by others.[370] The majority of cybercrime victims report emotional challenges, ranging from annoyance to depression, insomnia, anxiety, and panic attacks.[371]

---

[367] UN Women "The views expressed in this publication are those of the authors and do not necessarily represent the views of UN Women, the United Nations or any of its affiliated organizations." (2019) Safe Digital Spaces: Protection of Women and Girls from Technological Violence from http://africa.unwomen.org/en/digital-library/publications (accessed on 4 March 2023).

[368] Bossler, A., T.J. Holt, C. Cross, & G.W. Burruss: 2019. Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness.

[369] Nurse JR: 2019. Cybercrime and you: how criminals attack and the human factors that they seek to exploit.

[370] Button M, Sugiura L, Blackbourn D, et al. (2020) *Victims of Computer Misuse: Main Findings*. Portsmouth: University of Portsmouth.

[371] *Nature of Crime: Fraud and Computer Misuse - Appendix Tables*. Year ending March 2020. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefrau

South Africa at present is not equipped with a well-detailed cyber police strategy in place, nor does it have a coordinated approach in dealing with Gender Based forms of Cybercrime.[372] There is a shortage of specialized police officers trained to handle cyber-related crimes. This manifests in various ways, including a failure to collect evidence provided by the victim, inadequate support, advice, and updates on investigations, and a general lack of knowledge and awareness regarding the threat and risk faced by victims. Police officers often struggle to understand individuals who primarily operate online, leading to personality clashes during interviews with suspects and victims. Without a thorough understanding of the digital environment in which cybercrime victims and perpetrators operate, officers may struggle to comprehend their personal needs and circumstances.[373] The absence of political will to invest resources and training to combat this, together with an inadequate administrative system and a weak rehabilitation system, does not act as a deterrent; it allows for the development of Gender- based forms of cybercrime in society.[374]

Initial investigations include interviewing victims and witnesses, affirming that their needs are met, identifying suspects, scrutinising crime scenes, identifying additional possible sources of evidence, and documenting and submitting all pertinent records and intelligence gathered to the control prosecutor to examine the docket for prosecution.[375] However, with Gender-based forms of Cybercrime investigations, this process is not only hindered by the lack of knowledge regarding Gender-based forms of Cybercrime, coupled with the anonymity of suspects (and often victims), lack of understanding by the investigators of these individuals and the impact on their personal lives and the difficulty of the non-physical nature of the Internet itself.[376]

Furthermore, the cost of training law enforcement personnel to combat cybercrime is high.[377] Once trained, officers must keep their knowledge current to keep up with technological innovation. Aside from training the costly specialist software and technological equipment needed for forensic investigation, the police department must prepare for the possibility that some of the

dandcomputermisus

[372] M. Grobler, J. Van Vuuren. J. Zaaiman, *Preparing South Africa for cybercrime and cyber defense*. (2013)

[373] Her Majesty's Inspectorate of Constabulary (HMIC) (2015) Real Lives, Real Crimes: A Study of Digital Crime and Policing. Justice Inspectorates. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

[374] CL Ezeji, AA Olutola and PO Bello, 'Cyber-related crime in South Africa: extent and perspectives of state's roleplayers.' (2018) 31 (3) *Acta Criminologica: African Journal of Criminology & Victimology*, 93-110.

[375] College of Policing (2020) Investigation Process. Retrieved from: https://www.app.college.police.uk/app-content/investigations/investigation-process (Accessed 1 September 2023).

[376] Ibid.

[377] P Hunton. 'The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation.' (2011) 27 (1) *Computer Law & Security Review*, 61–67.

cases may include international boundaries and that significant funding may be needed for all elements of the investigations.[378]

The landscape of modern cybercrime investigations is marked by the intricate challenge posedby digital evidence, often encrypted or stored across various jurisdictions. Gender-based forms of Cybercrime require a specialized skill set that not all law enforcement personnel possess. As a result, crucial digital evidence is sometimes mishandled, overlooked, or compromised during the initial stages of an investigation due to a lack of knowledge and understanding. Digital evidence can also be quickly altered or erased, making it challenging to establish prima facie proof for further investigation, hampering the pursuit of justice for potential victims of Gender-based forms of Cybercrime.[379]

In our healthcare and educational system, young individuals often experience a prevalent bias and are often met with judgment from medical and educational professionals when they seek educational advice or treatment concerning sexual reproduction and rights and responsibilities. Additionally, there is a noticeable gap in the system's educational content concerning protected legislation around sexual health and intercourse, including sex workers and the LGBTQ community. This deficiency is worrisome, as it hinders the advancement and execution of sexual responsibilities and rights, leaving many victims of Gender based forms of Cybercrime feeling anxious and unwilling to seek help or report their experiences at educational and healthcare facilities.[380]

IV. THE IMPLEMENTATION, REPORTING, AND ENFORCEABILITY CHALLENGES FACED WITHIN CYBERCRIME AND GBV

The growing threat of cybercrime and GBV poses significant threats to South Africa. Due to the sophisticated methods of committing cybercrime and GBV, implementation, reporting, and enforceability have become more demanding. National and international law enforcement are faced with unique challenges due to cybercrime. To begin with, cybercrime may occur anywhere in the world and at any time; it affects a broader spectrum of people than traditional crime.

[378] Murali, S. (n.d.). KPMG INTERNATIONAL Issues Monitor Cyber Crime – A Growing Challenge for Governments Volume Eight. (

[379] P Casey, *Digital Evidence and Computer Crime*,2004, 12

[380] Soulcity.org.za. 2021. [online] Available at: <https://www.soulcity.org.za/campaigns/gbv/resources/understanding-gender-policy-and-gender-based- violence-in-south-africa-a-literature-review> [Accessed 17 September 2023].

Cybercrime is the term for illegal activity carried out through computers, networks, or the internet. It covers various unlawful behaviours, including hacking, identity theft, malware attacks, phishing and cyberbullying. Cybercrime implementation issues are numerous and diverse. The following are some of the principal difficulties:

a. Complexity of cybercrime

Cybercrime is a complicated phenomenon incorporating cutting-edge technology, cunning strategies, and an international criminal network. Cybercrime demands particular knowledge and abilities for both investigation and prosecution. Despite being discovered with hacking software while hacking into an organization system and arrested, no present statute allows for the prosecution of the individual[381]. If it can be demonstrated that the criminal personally benefited from their actions, they may have to face further charges such as theft. Therefore, safeguarding society from online threats becomes even more challenging. Law enforcement's primary task is to change how the general public views cybercrime, reduce their fear and strengthen the community's fortitude and preparedness. Any effort to secure cyberspace must focus on raising public awareness of cybersecurity issues and strengthening police capabilities.[382] In contrast to developing countries, developed nations have launched national cybersecurity Programmes to cultivate a culture and business environment that is educated about how to defend themselves from cyber-related threats.

b. Jurisdictional issue

Since cybercrime is frequently committed across international borders, it can be challenging to determine which country has jurisdiction over the crime. Investigations and prosecutions can be delayed as a result, and it might potentially provide legal difficulties. Given cybersecurity's international nature, every country must have a clear plan for educating its citizens on cybersecurity. The Cybercrimes and Cybersecurity Bill in South Africa was approved by the National Council of Provinces on July 1, 2020, which now awaits President Cyril Ramaphosa'sto sign it into law if he has any concerns about its Constitutionality, a possible referral back to

[381] KS Choi, *Cybercriminology and digital investigation* (2015).
[382] N Akdemir, B Sungur, and BU Basaranel 'Examining the Challenges of Policing Economic Cybercrime in the UK'(2020) *Guvenlik Bilimleri Dergisi*.

the National Assembly for further consideration.[383] The Cybercrimes and Cybersecurity Bill was passed on August 28, 2015, modified on January 19, 2017, and presented to parliament on February 22, 2017.[384] Every year, millions worldwide become victims of internet fraud, including dating site scams, online shopping fraud, gaming fraud, and responding to phoney e-mails requesting bank account information. When the Bill becomes law, it aims to do away with these difficulties and make it possible to enforce laws specific to cybercrime by prosecuting offenders.

c. Lack of resources

Cybercrime investigations demand a lot of resources, such as finance, qualified employees, and specialized equipment. Many law enforcement organizations lack the tools to investigate and criminalize cybercrime efficiently. The existing technological infrastructure in South Africa has several problems, such as the standardization or monoculture of operating systems.[385] As countless individuals to small and medium-sized enterprises use Microsoft's operating system, attackers may organize successful attacks by concentrating on just one target. The modern, sophisticated computers available on the market can be utilized to further criminal operations.[386] However, investigation issues are not solely brought on by the rising capabilityof single-user computers. Growing network capabilities is another critical problem. Most of the time, computers have malicious software installed that infects them and installs tools that allow offenders to seize control. With botnets, sophisticated assaults may be carried out, or targets can be profiled.[387] Botnets provide many benefits for criminals. They increase criminals' computer and network capabilities. Criminals can assault computers that would be inaccessible if only a few machines were used to spearhead the attack by using thousands of computer systems. Botnets also make it more challenging to find the original perpetrator because early leads only lead to botnet members.[388] The gap between the capabilities of investigative authorities and those under the control of criminals is widening as criminals gain

[383] REPUBLIC OF SOUTH AFRICA (2015) Cybercrimes and Cybersecurity Bill: Draft for public comment. Online Available from http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.
[384] C Cross (2019) Online fraud. Available from https://eprints.qut.edu.au/127162/
[385] Regarding the discussion on the effect of the monoculture of operating systems on cyberscecurity, see Picker, Cyber Security: Of Heterogeneity and Autarky, available at:http://picker.uchicago.edu/Papers/PickerCyber.200.pdf;Warning: Microsoft Monoculture, Associated Press,15.02.2004, available at www.wired.com/news/privacy/0,1848,62307,00.html.
[386] Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).
[387] Botnets as a vehicle for Online Crime (2005), available at: www.cert.org/archive/pdf/Botnets.pdf;Barford/Yegneswaran
[388] "How to Own the Internet in Your Space Time" (2002), available at:www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

control of increasingly potent computer systems and networks.

d. Rapidly evolving speed of data exchange technology

Cybercriminals continuously create new strategies and tools to stay undetected and carry out their activities. Law enforcement authorities must stay current with these advances to investigate and prosecute cybercrime successfully. It simply takes a few seconds to send emails and texts between nations. E-mails have reduced the need for physical delivery of a message, which is why the Internet has succeeded. However, due to the transfer speed, law authorities have little opportunity to conduct an investigation or gather evidence[389]. Traditional investigations need far more time to conduct or gather data. Internet-specific tools and instruments are needed for competent authorities to conduct investigations in order to investigate and prosecute cybercrime.[390] In this situation, it is crucial to have tools for locating the perpetrator and gathering the evidence needed for the criminal procedures. These tools might be the same in conventional, non-computerized terrorism investigations. Traditional investigative tools, however, are becoming insufficient to identify an offender in situations using the Internet. Consequently, developing new technology solutions and corresponding legal frameworks is vital.

e. Limited international cooperation

International collaboration is required to investigate and prosecute cybercrime effectively. The rules and regulations governing cybercrime vary from nation to nation, and certain nations can be reluctant to comply with investigations. Various data transmission procedures impact morethan one nation.[391] If direct links are momentarily prohibited, the protocols for Internet data transfers are based on the best possible routing[392] Even when domestic transfer procedures inside the source nation are restricted, data can leave the nation, travel via routers outside the nation, and then be rerouted back inside the nation to its intended location.[393]

[389] M Gercke 'The Slow Wake of a Global Approach Against Cybercrime' (2006) 140 *Computer Law Review International*

[390]."Urgent measures for combating international terrorism" Decree-Law (27 July 2005)No. 144

[391] Regarding the extent of transnational attacks in the most damaging cyberattacks, Cybercrime and Security- The Transnational Dimension in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, available at: http//media.hoover.org/documents/0817999825 1.pdf.

[392] The fisrt and still most important communication protocols are Transmission Control Protocol (TCP) and Internet Protocol (IP).

[393] 'Fighting Cyber Crime and Terrorism; The Role of Technology' presentation at the Stanford Conference, December 1999. The Transnational Dimension of CyberCrime and Terrorism, 2001 available at

Furthermore, many Internet services are reliant on foreign services. For instance, host providers may rent out webspace in one nation based on hardware in another. Cybercrime investigations require the collaboration of law enforcement authorities in all involved countries when offenders and targets are situated in various nations.[394] Investigations conducted without the consent of local authorities are prohibited under national sovereignty on the territory of other nations. All participating nations' authorities must assist and participate in cybercrime investigations. It is challenging to establish reciprocal legal assistance standards for collaboration in cybercrime.[395]

Investigations are typically hampered by the formalities and time needed to work with foreign law enforcement authorities. Inquiries frequently take place in incredibly short amounts of time.[396] Frequently, data that is essential for locating criminals is destroyed quickly. Offenders may pick their targets consciously and operate from nations with insufficient cybercrime laws. It would be beneficial to have international collaboration and harmonize the rules about cybercrime. The G8 24/7 Network and the requirements for international collaboration in the Council of Europe Convention on Cybercrime are two methods to increase international cooperation in cybercrime investigations. This limited investigation time is an issue since a conventional system of mutual legal help sometimes requires planning.

f. Difficulty in collecting evidence

Digital evidence may be encrypted or housed on servers across multiple jurisdictions, making collection challenging. Digital evidence can also be quickly altered or erased, making it difficult to establish the guilt of cybercriminals.[397] The handling of digital evidence presents unique difficulties and calls for specific protocols. The integrity of the digital evidence is one of the most challenging issues. Digital information is exceptionally brittle and quickly modifiable. This is particularly important for data that needs specific preservation methods since it is stored in the system memory RAM and immediately erased when the machine is shut

http://media.hoover.org/documnets/0817999825_1.pdf.

[394] National Sovereignty is a fundamental principle in International Law. See Roth 'State Sovereignity, International Legality and Moral Disagreement' (2005) available at www.law.uga.edu/intl/roth.pdf.

[395] M Gercke 'The Slow Wake of a Global Approach Against Cybercrime' (2006) 140 *Computer Law Review International* 142.

[396] Regarding the extend of cross-border cases related to computer fraud, see Beales, "Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging" (2004) available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[397] E Casey *Digital Evidence and Computer Crime*, 2004 12; F Insa 'The admissibility of Electronic evidence in court: fighting against high-tech crime' (2005) Cybex, available at: www.cybex.es/agis2005/elegir idioma pdf.htm.

down[398] Innovations can also significantly affect how we handle digital evidence. Cloud computing is one instance. When looking for computer data in the past, detectives may concentrate on the suspects' locations.[399] They now have to consider the possibility that digital material may be kept abroad and only accessed remotely when necessary.

g. Costly investigative procedure

Due to widespread ignorance of the dangers posed by cybercrime, many people may fail to take the appropriate safety measures. This may facilitate the commission of crimes by cybercriminals. The absence of funding for the investigation is a significant setback. The cost of training law enforcement personnel to combat cybercrime is high.[400] Once trained, they must keep their knowledge current to keep up with technological innovation. Aside from training, the costly specialist software and technological equipment needed for forensic investigation. The police department must prepare for the possibility that some cases may include international boundaries and that significant funding may be needed for all elements of the investigations.[401]

Cybercrime presents significant implementation challenges due to its complexity, jurisdictional issues, lack of resources, rapidly evolving technology, limited international cooperation, difficulty collecting evidence, and lack of public awareness. Addressing these challenges willrequire collaboration and cooperation between law enforcement agencies, governments, and the private sector. The following section shall discuss the challenges of reporting cybercrime.

h. Reporting cybercrime

In order to stop and combat such operations, reporting cybercrime is crucial. However, for a variety of reasons, reporting cybercrime can be complex. The primary reporting of cybercrime draws attention to individuals' significant difficulties when reporting incidents related to cybersecurity. The ability of individuals to identify and respond to cyber threats swiftly may

[398] Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: Moore'To View or not to view: Examining the Plain View Doctrine and Digital Evidence' (2004) 29 (1) *American Journal of Criminal Justice*.
[399] Moore'To View or not to view: Examining the Plain View Doctrine and Digital Evidence' (2004) 29 (1) *American Journal of Criminal Justice*.
[400] "Cybercrime presents a major challenge for law enforcement" EUROPOL, January 3,2011.
[401] KPMG 'Cyber Crime- A Growing Challenge for Governments' July 2011

be compromised without efficient incident reporting; it is crucial to note. In order to overcome these obstacles, the Republic of South Africa's government must prioritise creating efficient incident reporting procedures. In the present digital environment, effective incident reporting is essential for enterprises when cybersecurity incidents are becoming more frequent. It is recommended that organizations spend money on cybersecurity training and instruction for their personnel to provide them with the knowledge and abilities to spot and report incidents.

i. Fear of retaliation

Cybercrime victims could be reluctant to come forward because they are worried about the criminal taking revenge. In order to terrify their victims, cybercriminals may employ various strategies, such as making threats to expose their data or initiate new attacks. South African government should also strive to create transparent reporting processes that consider any internal policies or guidelines and legal and regulatory needs. Overall, documenting cybersecurity events is a complex process that necessitates much work and commitment from organizations.

j. Lack of awareness

Many people may be ignorant of the many forms of cybercrime or the available reporting options. They could be unaware that they have been a victim of cybercrime, or they could be unsure of how to file a report. Given the hazy tasks that monitoring professionals must play, the dearth of human and material resources, and the absence of employee feedback, ambiguous legal provisions are the root causes of corruption.

The inherent anonymity of the internet creates a practical enforceability challenge for law enforcement officers to ascertain the real identities of unknown individuals by solely relying on their online persona.[402] As a result, investigators cannot obtain statements from victims or witnesses, identify potential evidence sources (such as personal data, hard drives, or computers), or otherwise advance the investigation.[403] With gender-based forms of Cybercrime, safeguarding the victim by identifying and addressing the needs of the victim in order to prevent future victimisation can be challenging due to the lack of available support resources and inherent anonymity.

[402] C Dodge, G Burruss *Policing cybercrime* (2019)
[403] College of Policing (2020) "Investigation Process."

The landscape of modern cybercrime investigations is marked by the intricate challenge posedby digital evidence, often encrypted or stored across various jurisdictions. Gender-based forms of Cybercrime require a specialized skill set that not all law enforcement personnel possess. As a result, crucial digital evidence is sometimes mishandled, overlooked, or compromised during the initial stages of an investigation due to a lack of knowledge and understanding. Digital evidence can also be quickly altered or erased, making it challenging to establish prima facie proof for further investigation, hampering the pursuit of justice for potential victims of Gender-based forms of Cybercrime.[404]

The inherent anonymity of the internet creates a practical enforceability challenge for law enforcement officers to ascertain the real identities of unknown individuals by solely relying on their online persona.[405] As a result, investigators cannot obtain statements from victims or witnesses, identify potential evidence sources (such as personal data, hard drives, or computers), or otherwise advance the investigation.[406] With gender-based forms of Cybercrime, safeguarding the victim by identifying and addressing the needs of the victim in order to prevent future victimisation can be challenging due to the lack of available support resources and inherent anonymity.

V. CONCLUSION

In conclusion, examining the Cybercrimes Act in South Africa reveals a commendable effortin addressing various cybercrimes, yet it falls short in explicitly considering and penalizing gender-based cybercrimes. Gaps are identified in Sections 2 to 12, emphasizing the need for

explicit language to address unique nuances, especially in offences like sextortion. Despite recognizing the Act's positive aspects, there is a pressing call for refinement and inclusion of provisions explicitly targeting gender-based cybercrimes within the legislative framework. The chapter concludes by urging the interpretation of the Act to allow regional magistrates to issue search and seizure warrants, emphasizing the importance of unified and effective responses to cyber threats.

[404] E Casey *Digital Evidence and Computer Crime*, 2004 12; F Insa 'The admissibility of Electronic evidence in court: fighting against high-tech crime' (2005) Cybex, available at: www.cybex.es/agis2005/elegir idioma pdf.htm.
[405] C Dodge, G Burruss *Policing cybercrime* (2019)
[406] College of Policing (2020) "Investigation Process". Retrieved from: https://www.app.college.police.uk/app-content/investigations/investigation-process (Accessed 13 September 2023).

The analysis emphasizes the delicate balance between addressing gender-based cybercrimes promptly and safeguarding individual rights. Noteworthy innovations, such as oral applications in urgent situations, are acknowledged, but potential vulnerabilities in the absence of explicit considerations for gender-based cybercrimes in oral warrant applications are identified. The Act's provisions on execution of search warrants, limitations on specialized tools, international cooperation, and capacity building contribute positively, yet gaps are highlighted, urging explicit inclusion of gender-specific considerations in training and reporting mechanisms. The chapter concludes by aligning the Act with the National Strategic Plan on GBVF, suggesting potential enhancements and dedicated legislation for gender-based cybercrimes to ensure comprehensive protection.

CHAPTER FOUR: RECOMMENDATIONS AND CONCLUSIONS ON HOW TO COMBAT GBV CYBERCRIMES.

I. INTRODUCTION

In this chapter, the findings and recommendations of the study are thoroughly examined, offering valuable insights into the complex intersection of cybercrime and GBV. Through meticulous analysis, the study identifies critical challenges and areas for improvement in addressing gender-based cybercrimes, both at the national and international levels. Practical recommendations are provided for policymakers, law enforcement agencies, and relevant stakeholders to enhance victim protection, improve law enforcement competency, and foster interdisciplinary collaboration in combating these crimes effectively. In conclusion, the study underscores the importance of concerted efforts to address gender-based cybercrimes and emphasizes the need for ongoing collaboration and innovation to create a safer online environment for all.

II. SUMMARY OF FINDINGS

a. Existing international and regional frameworks pertaining to cybercrime and GBVresponse

The analysis of existing international and regional legal frameworks reveals several key findings. Firstly, the increasing Internet penetration across Africa has heightened susceptibilityto cybercrimes, including gender-based forms. This underscores the urgent need for cybersecurity awareness and training to mitigate risks and protect users. Additionally, UN mandates and efforts, led by entities like the United Nations Special Rapporteur on Violence Against Women and UN Women, actively address GBV in cyberspace. These initiatives aim to create a safer online environment through reports, recommendations, and advocacy for legal reforms. Moreover, international conventions such as CEDAW and the Beijing Declaration recognize the intersection between GBV and technology. By providing frameworks for combating online GBV, these conventions contribute to shaping global responses to cybercrimes. However, challenges persist regarding the adequacy of specific legal instruments.

For instance, while the Budapest Convention has influenced domestic legislation in South Africa, concerns remain about its ability to address emerging forms of gender-based cybercrimes effectively. Furthermore, the Malabo Convention seeks to harmonize cybersecurity laws in Africa, but obstacles such as more significant ratification and legislative

adaptation hinder its full potential. Particularly concerning is the need to address gender-specific cybercrimes comprehensively within this framework.

b. Current legislative framework governing cybercrime forms of GBV in South Africa

In the context of South Africa, legal frameworks such as the Constitution and the Cybercrimes Act provide a foundation for combating cybercrimes. The Constitution stipulates that every citizen is equal before the law and has the right to equal protection and benefit from the law. This section protects against gender-based forms of cybercrime using any kind of electronic communication. It accomplishes this by ensuring that women are not discriminated against, abused, or sexually harassed online because of their ethnicity, gender, sex, colour, or religion. The harsh reality is that it has taken the government 20 years since the enactment of the Electronic Communications and Transactions Act 25 of 2002 (ECT) to implement legislation that guarantees the Constitutional right of protection for women who have previously been denied protection against Gender-Based Forms of Cybercrime. Examining South Africa's Cybercrimes Act demonstrates a remarkable effort to address numerous cybercrimes, but it fails to expressly identify and penalise gender-based cybercrimes. Sections 2–12 identify gaps, emphasising the importance of specific wording to address unique complexities, particularly in offences such as sextortion. Despite the Act's excellent characteristics, there is a strong desire for its refining and inclusion of provisions that clearly address gender-based cybercrimes within the legislative framework. POPIA and RICA in South Africa play crucial data protection and surveillance roles, respectively. While these laws have implications for combating gender-based cybercrimes, there is a pressing need for more precise provisions and enforcement mechanisms to address specific challenges in this domain. International cooperation, legal reforms, and awareness campaigns are essential components of a comprehensive strategy to address gender-based cybercrimes within existing legal frameworks effectively.

c. The implications for strengthening South Africa's response to cybercrime and GBV

The analysis highlights a pressing need for South Africa to refine its legislative framework to explicitly address gender-based cybercrimes within existing laws. Despite foundational provisions within the Constitution, identified gaps in the Cybercrimes Act and related legislation necessitate specific amendments to effectively combat such crimes. Through synthesizing previous chapters' findings, it becomes evident that South Africa's response to cybercrime and gender-based violence (GBV) remains inadequate in meeting international obligations and constitutional protections. While the Constitution provides a solid foundation,

it falls short of offering comprehensive safeguards against evolving cyber threats targeting women and girls. Existing legal responses lack the necessary strength to adequately protect vulnerable populations and uphold individual rights to privacy and freedom of expression.

The research underscores the urgency for South Africa to align its legislative framework with international conventions and constitutional mandates to effectively address cybercrimes and GBV. Despite some efforts to integrate international best practices, such as the ratification of relevant treaties, the current legal landscape falls short of providing robust protection against gender-based cybercrimes. Specific amendments to the Cybercrimes Act and related legislation are imperative to close existing gaps and enhance enforcement mechanisms. Moreover, a stronger stance is needed to ensure compliance with international obligations while safeguarding individual rights guaranteed by the Constitution.

III. RECOMMENDATIONS

The landscape of cybercrime is rapidly evolving worldwide, presenting significant challenges for law enforcement in combating illicit online activities. Particularly vulnerable to these threats are women and children, who often fall victim to various forms of cybercrime, including sexual harassment and exploitation. Consequently, there is an urgent need to implement comprehensive measures, regulations, plans, and programmes to address this growing criminal phenomenon effectively. To combat gender-based cybercrimes effectively, it is essential to address key factors such as political, behavioural, and economic aspects, fostering a culture that staunchly opposes GBV and consequently reduces cybercrimes perpetuating this harmful culture.

a. Policy implementations

The Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, along with the Optional Protocol to the Convention on the Rights of the Child concerning the sale of children, child prostitution, and child pornography, as well as online violence against women, require acknowledgment followed by concrete legal provisions. [407] CEDAW is consequently not critical enough when it comes to women facing the atrocities mentioned above. An encouraging legislative enactment can be found in the Romanian Law, which 'modifies and completes law' regarding preventing and combating domestic violence.[408]

[407] R Almenar, 'Cyber violence against women and girls: GBV in the digital age and future challenges as a consequence of Covid-19' (2021) available at https://teseo.unitn.it/tslr/article/view/757/337
[408] Ibid.

This highlights the need to address GBV forms of cybercrimes within existing legal frameworks. While international conventions such as the Lanzarote Convention and the Optional Protocol to the Convention on the Rights of the Child acknowledge the importance of combating online violence against women and children, they require further reinforcement through concrete legal measures. The example of Romania's legislative response to cyber domestic violence underscores the importance of institutionalizing the concept of GBV and cybercrimes within national legal frameworks.

This law was adopted following the 'ruling against Romania by the European Court of Human Rights in the *Buturuga v Romania* case; here, it was found that Romania had failed to take into consideration the various forms that domestic violence can take, referring to cyber GBV'. [409] However, even this is not entirely adequate regarding GBV forms of cybercrimes because the main focus is on domestic violence that is cyber.[410] It is recommended that South Africa include definitions and measures related to GBV cybercrimes in existing legislation addressing sexual offences and domestic violence. This entails amending relevant laws to explicitly recognize and address the various forms of cybercrimes that disproportionately affect women and girls. Additionally, there is a need for policies and interventions that specifically target GBV cybercrimes, including initiatives aimed at raising awareness, providing support for victims, and enhancing law enforcement responses. By incorporating GBV cybercrime definitions and measures into existing legislation and policies, South Africa can take a proactive step towards effectively addressing this critical issue.

Suggestions have been made that the South African government, in collaboration with social media researchers and developers, should establish social media policies aimed at imposing strict penalties on individuals who utilize social media platforms to perpetrate online gender-based violence against women.[411] Many South Africans who use social media have an inclination to be influenced by public opinion, and if social media sites do not put measures inplace to mould the digression of information on their sites, then it can be unsavoury used to promote 'and legitimize acts of GBV such as intolerance, distrust and hate'.[412] It is recommended that the South African government takes proactive steps to develop and implement social media policies aimed at combating online GBV against women. These policies should be developed in collaboration with social media researchers, developers, and

[409] Ibid.
[410] Ibid.
[411] Ibid.
[412] Ibid.

relevant stakeholders to ensure their effectiveness and feasibility. Social media platforms have a responsibility to implement measures that prevent the dissemination of harmful content and punish instigators who use their platforms to perpetrate GBV. As part of these policies, social media platforms should be required to implement mechanisms to monitor and remove content that promotes or legitimizes acts of GBV, such as intolerance, distrust, and hate speech. Additionally, platforms should be obligated to enforce strict penalties for individuals found guilty of instigating GBV online, including banning offenders from their platforms and cooperating with law enforcement authorities in prosecuting perpetrators.

Usually, ICT policies are gender-blind and fail to focus on how women and men are affected.[413] A specific focus on violence against women and girls is less catered for in the cyber realm of interactions.[414] Efforts to combat ICTs that exploit and abuse women and children are paramount and must be genuine. Thus, governments and national authorities should prioritize a women and child protection approach that unequivocally upholds human rights. This entails continuously updating legislation to keep abreast of technological advancements, as well as recruiting, training, and retaining specialized personnel. Additionally, gaining access to cutting-edge technological resources and establishing effective mechanisms for accessing third-party data and conducting undercover investigations are essential components of this endeavor.[415]

Policies must also be developed to provide guidance on harmful online conduct committed bythe youth.[416] These policies need to be formulated through a multidisciplinary approach that incorporates 'best practices from social science, legal policy and public policy'.[417] Laws that currently deal with ICT-related crime need to account for gender differences and inequalities in areas that cover topics where women are deeply affected, such as 'privacy laws and pornography laws'.[418] Addressing harmful online conduct by youth, particularly considering gender differences and inequalities in areas like privacy and pornography laws, should be incorporated into the Cyber Crimes Act. The Act should encompass provisions derived from a multidisciplinary approach, integrating insights from social science, legal policy, and public policy to effectively address such issues within its framework. This ensures

[413] UN Women *Safe Digital Spaces: Protection of Women and Girls from Technological Violence* (2020) available at https://africa.unwomen.org/sites/default/files/Field%20office%20Africa/Attachments/Publications/2020/Backgroundpaper.Webpdf (accessed on 28 June 2023)
[414] Ibid.
[415] Ibid.
[416] Ibid.
[417] Ibid.
[418] Ibid.

comprehensive coverage and responsiveness to evolving challenges in the digital realm, safeguarding individuals from various forms of cyber-related harm.

To ensure a comprehensive perspective on 'technology-related violence against women, 'inter-thematic dialogue and research with a range of actors, from women's rights advocates to state actors and private companies, which covers the range of issues that affect women's rights and ICT, is necessary.[419]

Different forms of cyber GBV offences carry varying degrees of harm for the victim to heal from. Therefore, the greater the probable damage to a victim, 'the greater the precautions that the intermediary should employ when developing and applying their terms and conditions of service, community standards and codes of ethics'.[420] This needs to happen whilst keeping in mind the need to prevent the expansion of abusive imagery and language that plant seeds of gender hatred and seek to incite violence.[421] It has been suggested that 'internet intermediaries' should regularly conduct 'due diligence assessments of their compliance with the responsibility to respect human rights and fundamental freedoms'.[422] The government can make this a mandatory requirement for internet intermediaries to ensure that stats and yearly reports are provided regarding cyber GBV incidents and how these have been dealt with. There are victims of 'non-consensual creation, publication, divulgation and reproduction of offending, degrading and illicit contents, both verbal and non-verbal'. This is instigated by perpetrators who circulate the information mentioned above all over social media, and this can create a 'stereotyped image of women and girls', which dilutes the value of their empowerment in a digital space.[423]

The inclusion of legal prohibitions against online divulgation, supported by modern algorithms, could be effectively enacted within the Cybercrime Act. Specifically, amendments or additions to the Act could introduce provisions targeting the dissemination of sensitive or private information online without consent, utilizing algorithmic detection mechanisms to identify and address such violations. This integration would enhance the Act's capacity to combat cyber-related offenses, ensuring greater protection of individuals' privacy and mitigating the proliferation of harmful online content.

[419] Ibid.
[420] L Bassan *Cyberviolence as Violence Against Women and Girls : Taking a step forward for Female inclusion in the Digital Era* (LLM thesis, Ca'Foscari University of Venice, 2004).
[421] Ibid.
[422] Ibid.
[423] Ibid.

b. Enhancing law enforcement competency and interdisciplinary collaboration forcombatting gender-based forms of cybercrime

As noted in earlier chapters, key impediments to addressing cyber-criminal activity include the gaps in the activities of inquiry and preliminary investigation. To effectively combat this challenge, this study recommends implementing comprehensive training Programmes for law enforcement personnel focused on cybercrime detection, investigation, and evidence collection techniques. Additionally, there should be increased collaboration and information-sharing mechanisms among relevant agencies, both domestically and internationally, to enhance the efficiency and effectiveness of cybercrime investigations. Furthermore, allocating sufficient resources, including funding and personnel, to cybercrime units within law enforcement agencies is essential to ensure that they have the capacity and expertise to effectivelyinvestigate and prosecute cybercriminals. By addressing these impediments and implementing the recommended measures, law enforcement agencies can enhance their capabilities in combating cybercriminal activity and safeguarding individuals and organizations from online threats.

An investigation method offered by a criminological analysis study on determinants of cybercrime technologies suggests that using a methodological basis that contains 'complex comparative analysis and statistical data analysis in the cybercrime field while also including 'interdisciplinary analysis yields good results.[424] It has been found that the benefits of this proposed investigation method 'are based on combining methods of one sphere (Criminology) with other spheres (cyberspace)'[425] this allows for an accurate description of the reality of cybercrimes and how to engage in its prevention. Therefore, there needs to be an interdisciplinary approach cultivated when it comes to the prevention and reduction of Gender Forms of Cybercrime by including fields like psychology that are focused on why there is this occurrence of GBV online and having law enforcement become highly engaged in this frontier.

Given the transnational nature of cybercrime, traditional law enforcement tools are often ineffective in combating online crimes that involve victims and perpetrators in different jurisdictions.[426] To address this challenge, it is recommended to establish a robust information infrastructure through collaboration with industry stakeholders, internet users, and even ethical hackers. By leveraging the expertise and resources of these stakeholders, law enforcement

[424] Ibid 1133.
[425] Ibid.
[426] F Cassim 'Formulating specialised legislation to address the growing spectre of cybercrime : a comparative study' (2009) 12(4) *Portchefstroom Electronic Law Journal* available at

agencies can enhance their capabilities in detecting, investigating, and prosecuting cybercriminal activities that span across borders. This collaborative approach allows for the sharing of intelligence, technical expertise, and best practices, ultimately strengthening the global response to cybercrime and improving the protection of individuals and organizations from online threats.

The saying 'it takes one to know one' is a concept that can be utilized by law enforcement to catch internet offenders and hackers. Thus, enlisting hackers or ex-hackers to work with police and investigators would greatly help reduce the incidence of human trafficking, which is currently bolstered because of highly evolved technology that is presently accessible to anyone. Countries will be able to work together to solve cybercrime cases with the help of skilled personnel in a department dealing with cyberattacks and with the requisite hacking skills. Regarding obtaining the help of hackers, 'it is advocated that cybercrime policy should encourage their co-operation and avoid alienating them'.[427] South African Police Services canenlist hackers to join the force in helping combat cybercrimes, as this would be a helpful resource.

The South African government appears to be making strides in addressing the issue of GBV, but there is a pressing need to direct more attention towards Gender-Based Cybercrimes. Given its profound impact on the lives of victims, a focused approach is essential. While the path forward may pose challenges, incremental steps focused on analysis and action can greatly benefit future generations. Drawing inspiration from successful strategies implemented in other countries and leveraging insights from professionals in various disciplines can enhance our understanding of the GBV landscape and support cyber experts. Therefore, fostering a collaborative learning environment is imperative.

Tools and mechanisms exist to address gender-based cyber crimes effectively. Yet, fostering a unified and cooperative culture across Africa and globally is essential for sustainable and effective solutions. Collaborating with influential figures and world leaders can significantly contribute to creating a safe and inclusive cyberspace for all, ensuring gender equality and security in navigating the evolving technological landscape of the modern era.

Establishing forums to gather intelligence on suspected criminal activities online, like those recruiting cybercriminals, can aid law enforcement in identifying and dismantling these forums or criminal syndicates over time. There must be a united frontier created to combat GBV cybercrimes; hence, a task force or police department dedicated solely to these crimes is

[427] Ibid.

imperative, but as can be seen, having the facilities without proper knowledge and skill will not help get to the root of these violations. Law enforcement needs to be trained and skilled in line with the international best practices to stifle cybercrime and GBV.

c. Increase resources

As noted in chapter three studies indicate that a lack of resources poses another obstacle to effectively combatting cybercrimes.[428] This setback is linked to 'insufficient training and low- level knowledge about these emerging crimes and an inability to keep pace with technological advances.'[458] Police officers need to be more hands-on in working on cybercrime cases. S 57 of the Cybercrimes Act must be utilized to its full capacity, particularly s 57 subsections (1) (b) (c) (d) (e) and (f). Section 1(b) outlines cybercrime response activities, which must be executed swiftly and effectively to address GBV cybercrimes. Perpetrators of such crimes are notorious for their rapid and efficient actions. Therefore, it is crucial to ensure that cybercrime response activities are conducted promptly and efficiently to counteract these perpetrators' tactics effectively. S57 (1)(c) encourages 'training, research, information and technology-sharing' and promotes the exchange of information regarding the detection, prevention, mitigation and investigation of cybercrimes. To combat GBV cybercrimes, a focus-oriented guideline must be introduced to help law enforcement and the public understand the gravity and width of cybercrimes that are forms of GBV. This will allow more victims to come forward in the hope that law enforcement can help them, and by raising the number of victims that come forward, the statistics will increase, and this will aid with the necessary technological advancements needed to combat GBV cybercrimes

Section 57(1)(d) focuses on establishing points of contact to facilitate mutual assistance and cooperation regarding listed cyber offences. While the provision of such points of contact is crucial, it is important to consider integrating support for victims of cyber violations into existing spaces and centres rather than establishing new ones. Encouraging non-governmental organizations (NGOs) to include awareness and response to cybercrime violations in their existing Programmes can be an effective approach. Moreover, our national GBV Strategic Plan should incorporate measures for reporting, response, and support for victims of GBV cybercrime. This includes equipping South African Police Service (SAPS) and Thuthuzela

[428] S Yeop Paek and M K Nalla et al.. 'The perceived importance of cybercrime control among police officers: Implications for combatting industrial espionage'(2021) 13(8) *Industrial Security for Sustainable Technology Innovation and Economic Growth.*

Care Centres to effectively address these crimes by providing support for reporting, counseling, and legal remedies. By addressing the psychological stress and potential further harm experienced by victims, these centers can offer comprehensive assistance to those affected by GBV cybercrimes.

As noted in chapter three there is a lack of investigation units available to investigate cybercrimes; thus, the capacity to conduct successful investigations is weak.[429] In an article issued by Zizamele Cebekhulu-Makhaza (President of Police and Prisons Civil Rights Union), it is said that 'South Africa must develop a more comprehensive strategy' to tackle its cybercrime issues.[430] Investments into better technology, 'enacting more vital legislation, and building partnerships to enhance cooperation and information sharing among law enforcement agencies'[431] are required. South Africa can act adequately with the aid of international cooperation and countries to gain the funding necessary to acquire better technology and further develop the field of GBV cybercrimes, especially since it is currently at an all-time high. Additionally, the government should allocate and allocate its own funds towards initiatives aimed at addressing GBV cybercrimes in South Africa. This commitment is essential as it can elevate South Africa's profile internationally and attract global support for combating GBV cybercrime. By incorporating a strategic response to GBV cybercrimes into our national GBV strategic plan, we can effectively mobilize resources and coordinate efforts to address this pressing issue.

To effectively enforce cybercrime legislation, it is imperative to allocate significant resources, especially for cross-border investigations that require collaboration among law enforcement agencies across multiple countries. Adequate resources and cooperation from relevant authorities are essential for conducting successful international or transnational investigations. Therefore, the recommendation is to prioritize the allocation of resources towards enhancing cross-border collaboration mechanisms and providing necessary training and technical support to law enforcement agencies involved in cybercrime investigations. Additionally, establishing formalized partnerships and information-sharing agreements between countries can facilitate smoother cooperation and improve the effectiveness of international cybercrime investigations.

Statistics demonstrates that, in comparison to men, women encounter more severe consequences at the personal level as a result of cybercrime, cyber fraud, and cyber abuse

[429] Polity 'SAPS need resources and skills to fight cybercrime' 26th May 2023 available at https://m.polity.org.za/article/saps-need-resources-and-skills-to-fight-cybercrime-2023-05-26, accessed on 27 June 2023.
[430] Ibid.
[431] Ibid.

through tactics such as social engineering (e.g., sextortion, revenge porn, and cellphone stalking).[432] To promptly aid victims of gendered violence, the concept of Women Police Stations was introduced in India in 1970. Following this initiative, numerous women-only police stations have been established worldwide, including in countries such as Argentina, Bolivia, and Brazil, among others.[433] South Africa could attempt the facilitation of GBV desks staffed by women police officers at every station and review the statistics of GBV violence reports before and after its establishment. However, this should not be run entirely in isolation from men because to combat GBV cybercrimes, men and the youth adequately need to be heavily involved in these programmes and facilities that are created to raise awareness and tackle cybercrimes. These stations would feature specialized units staffed with trained officers knowledgeable about gender-based cybercrime and proficient in managing cases from initial complaint to conviction while ensuring the preservation of the victim's dignity. To enhance efforts in combatting online facilitated abuse and exploitation of women and children, it is crucial for governments and national authorities to prioritize several key aspects. Firstly, they should adopt an approach focused on protecting women and children while fully upholding human rights. This entails ensuring that legislation remains updated to address advancements in technology. Additionally, there is a need to recruit, train, and retain specialized personnel capable of dealing with these issues effectively. Access to state-of-the-art technological resources is essential, along with the development of efficient mechanisms for accessing third-party data. Policy development in this realm benefits from a multidisciplinary approach that integrates research findings and best practices from social science, legal studies, and public policy.

'There are some good advances in tools to fight cybercrime on the surface web and dark web'.[434] One such tool is 'Spotlight, ' which was created through a partnership involving Thorn and Digital Reasoning. This tool 'scraps publicly available information from the internet, analyses it and uses it to help prioritize cases for law enforcement'.[435] This program is focused on child trafficking data and aids with speeding up the police response time through the facilitation of 'concentrated data to work with'.[436] A Louisiana Lieutenant said that "seeing the spotlight in action reinforces the idea that we can use technology for good".[437] This tool presents a valuable

[432] Ibid.
[433] Ibid.
[434] L M Rhodes 'Human trafficking as cybercrime' (2012) *AGORA International Journal of Administration Sciences* 25 -26.
[435]Ibid.
[436] Ibid.
[437] Ibid.

opportunity for South Africa to address Gender-Based Forms of Cybercrime effectively. The state, specifically the SAPS and the National Prosecuting Authority (NPA), should take the initiative to seek authorization for the implementation of a tool similar to Spotlight. This tool, adapted to focus on Gender-Based Forms of Cybercrime, has the potential to significantly enhance efforts in combating such offenses. By partnering with international organizations or seeking collaborative assistance, South Africa can leverage this tool to provide crucial support to those affected by cyber-related GBV, thus reinforcing its commitment to protecting vulnerable individuals within the community.

d. Awareness programmes

The prevalence of cyber sexual violence underscores the urgent need for comprehensive measures within the legal framework, including the Cybercrime Act, to address and prevent such offenses. Given the significant impact on mental health and well-being, public education and awareness campaigns must be robust and multifaceted. State-led initiatives, like the inclusion of cyber sexual violence awareness in campaigns such as the 16 days of activism, can effectively raise awareness and reduce stigma surrounding these issues. Moreover, integrating education on cyber sexual violence into school curricula, as part of life orientation programmes, ensures early exposure and understanding among young individuals, fostering a culture of respect and consent online. NGOs play a crucial role in complementing these efforts through targeted advocacy, support services, and community engagement.

Women's experiences of violence may also be triggered by men feeling disempowered.[438] This happens because of a rapidly changing environment that involves social and economic foundations that impact the perceptions of women's and men's roles and rights within society. Campaigns can be started that encourage women to stand up for themselves and not accept male dominance at all costs; these campaigns must equally educate women on how not to feed the narrative that ends up with them suffering heinous GBV violations.

Integrating GBV awareness into school curricula could help counter the prevalent misogynistic narrative in South Africa, addressing the long-standing issue of female subjugation to male dominance evident throughout the country's history.[439] The offender retains the ability to

[438] E Warner and X Miedema et al.. 'Why do some men use violence against women and how can we prevent it? Multi-country study on men and violence in Asia and the Pacific' (2013) *United Nations Entity for Gender Equality and the Empowerment of Women.*
[439] S Essof 'South Africa:Violence against women and information communication technologies' (2009) *Association for Progressive Communications.*

monitor the victim, a tactic historically used to assert dominance. Changing societal attitudes towards women, deeply ingrained over time, is crucial. The government should promote school initiatives and awareness campaigns to foster an inclusive cyber environment that respects gender equality. After all, the youth is the future, and they need to be guided to plant the seeds of change that will reduce all forms of violence against women and children, thus making this phenomenon a taboo concept.

Providing comprehensive education to children in today's rapidly advancing technological landscape is essential, guiding them on responsible interaction with diverse media content they encounter. This proactive approach may serve as a preventive measure against future incidents of cyber-enabled GBV, instilling in young minds the importance of ethical online behaviour and discouraging paths that could lead to cybercrime or the perpetration of GBV.

Women and minors who post personal information regarding themselves on 'job and marriage websites or social networking websites are often at the receiving end of cybercrime'.[440] Vulnerable persons should refrain from posting highly personal information about their lives online as this opens the door to cybercriminals to use this information to manipulate one into working with them or simply attempting to violate and extort the victim.

To effectively shield women from media that perpetuates their objectification, governments and international bodies must collaborate earnestly and create online content that is pertinent and actively challenges sexist stereotypes[441] One strategy is to enlist influential personalities to advocate for a shift in the discourse surrounding GBV and cybercrimes. Collaborating with well-known figures whom young people admire can effectively raise awareness and educate them about the risks associated with consuming harmful content that portrays women negatively, such as pornography. The South African Constitution guarantees the right to freedom of artistic creativity. However, it is imperative to delineate boundaries to ensure thatthis freedom does not encroach upon the rights of others, particularly considering its impact on impressionable youth, who play a pivotal role in shaping the future of society.

Interventions with social media platforms are necessary to address their role in facilitating activities like connecting co-offenders or enablers within various networks.[442] Thus, criminals can easily manoeuvre through these forums and 'increase criminal capabilities of their

[440] L F Tatarinova and Karimzhan et al.. 'Criminological analysis of determinants of cybercrime technologies' (2016) 11(5) *IEJME-Mathematics Education.*
[441] N Agarwal and Dr N Kasuhik 'Cybercrimes against women' (2014) 4 (1) *Global Journal of Research in management* 37-49.
[442] Ibid.

networks quickly'.[443] This is especially true for loners who begin experimenting 'out of curiosity' with different legal or illegal technical tools and can thus end up in 'criminal networks through forums'.[444] Raising awareness about such activities is crucial for developing effective countermeasures, particularly within the SAPS. Well-known businesses can come forward and help fund awareness campaigns that will exacerbate the response rate of the South African government to take these factors into critical consideration because fully protecting women in the physical world from GBV does not prevent it from happening to them daily in the cyber world that almost everyone is looped into.

e. Safe havens

Based on findings in previous chapters regarding the inadequate state response to cybercrime, it is evident that the harmonization and enforcement of national, regional, and international laws are crucial in combating cybercrime effectively. Cybercrime safe-havens, which arise in countries lacking sufficient cybercrime legislation or where enforcement is lacking, pose significant challenges in prosecuting cybercriminals. These safe-havens thrive when there is a lack of alignment between national cybercrime laws or when enforcement is inconsistent. Therefore, it is imperative for South Africa to ensure that cybercrime safe-havens do not find refuge within its borders. This can be achieved through the alignment and enforcement of robust cybercrime laws at both national and international levels, thereby eliminating spaces for cybercriminals to operate with impunity.

Article 25 of the AU convention mandates member states to implement legislative and regulatory measures as they see fit, aimed at assigning particular responsibilities to institutions, whether newly established or existing. These measures also extend to designated officials within these institutions, granting them statutory and legal authority to address all facets of cybersecurity application.[445] In addressing the responsibility to protect women and girls from GBV cybercrimes, it is imperative to ensure that all aspects of cyber security applications encompass these forms of cybercrimes. This includes implementing measures to safeguard potential victims from online violations. Firewalls serve as a crucial first line of defense in preventing online trespasses and ensuring safe usage. Therefore, victims and potential victims should be advised to enable the firewall on their routers as a proactive measure to enhance their online security.

[443] L F Tatarinova and Karimzhan et al.. 'Criminological analysis of determinants of cybercrime technologies' (2016) 11(5) *IEJME-Mathematics Education* 1131.
[444] Ibid.
[445] Ibid.

However, in South Africa, there is a notable lack of comprehensive measures and awareness programmes specifically targeting GBV cybercrimes. To address this gap, it is recommended that the government implement targeted initiatives aimed at raising awareness about GBV cybercrimes and providing support and resources for victims. This may include developing educational campaigns, establishing support networks, and providing training for law enforcement personnel to effectively respond to GBV cybercrimes. Additionally, enhancing collaboration between government agencies, non-governmental organizations, and the private sector can facilitate a more coordinated and holistic approach to addressing GBV cybercrimes in South Africa.

f. Social media reform

Social media platforms have a responsibility to implement stricter policies and mechanisms for reporting and addressing cyber sexual violence, including proactive detection algorithms and user education initiatives. By mobilizing a coordinated approach across these sectors, society can work towards combating cyber sexual violence, promoting gender equity, and safeguarding the well-being of emerging young women.

In the context of South Africa, advocating for global social media companies to adopt specific safeguards and policies against cyber GBV is essential. Given the pervasive nature of online GBV and its detrimental impact on individuals' safety and well-being, concerted efforts are necessary to mitigate these risks. South Africa should actively engage with international partners and platforms to advocate for the implementation of robust policies tailored to address cyber GBV within online spaces. This advocacy could include pushing for measures such as enhanced reporting mechanisms, stricter content moderation policies, and proactive measures to prevent harassment and exploitation. By urging global social media companies to prioritize the protection of users from cyber GBV, South Africa can contribute to creating safer online environments and combatting the proliferation of harmful behavior on digital platforms.

Deriving from this point is that GBV online is especially dangerous because there is a lack of 'rules and regulations to protect women from this type of violence'.[446] Hence, platforms like Instagram, Twitter, Facebook, and other social media sites can adjust their protocols according to the regulations stipulated by their jurisdictions. These regulations may entail, for instance, a mandate for Instagram to establish a policy addressing GBV, wherein violators could face fines or

[446] N Sundani , A.C Mangaka and J Mamokhere 'Social media as a campaign tool against online GBV in South Africa (2022) *Science Rise* (5) 30-41.

imprisonment. Enforcing regulations mandating social media platforms like Instagram to establish policies addressing GBV would likely fall under the jurisdiction of regulatory bodies or government agencies responsible for overseeing telecommunications, internet, or digital media sectors. A careful consideration and coordination among relevant regulatory and enforcement authorities would be necessary to effectively enforce such regulations and ensure accountability within the online space. Consequently, Instagram would need to enhance its software capabilities to detect and monitor user activity that may constitute criminal behaviour. Social media companies should also maintain dedicated teams capable of promptly assisting users whose accounts have been compromised, preventing criminals from exploiting stolen identities for personal gain.

'Cyber Stalking' is a highly evolving cybercrime in the modern world.[447] This form of abuse can be used simultaneously with harassment, and it invades a person's privacy, such as their movement across the internet.[448] Social media sites can block this type of cybercrime by monitoring behaviours online that resemble the actions of an online stalker and then sending a notification to the user who is being allegedly stalked. The alleged victim can then follow up with the threat notification and request for it to be further investigated; in the meantime, the alleged victim's social media accounts should be suspended; this is an existing option available to social media account holders. This process would help prevent and tackle cyberstalking.

Gender-based forms of cybercrime are higher than ever presently and present a growing technological phenomenon for countries as noted in chapter two. Women and girls are the usual and most affected group of persons who face gender-based forms of attacks online. Therefore, social media companies and institutions are called to reformulate and add specific Programmes onto their systems to ensure a safer environment that exists free from gendered hate speech, sexism and overall unwanted overtures that women and girls experience.

IV. CONCLUSION

The analysis conducted in this study addresses the research questions posed regarding cybercrime forms of GBV in South Africa. Firstly, it critically examines the adequacy of the current legislative framework in addressing gender-based cyber violence and identifies implementation and enforcement challenges. Secondly, the study evaluates whether this framework effectively fulfils South Africa's obligations under international law provisions,

[447] Ibid.
[448] Ibid.

including treaties and conventions such as CEDAW and the Beijing Declaration. Thirdly, it explores the implications of the findings for strengthening South Africa's response to cybercrime and GBV.

The conclusion drawn from the analysis underscores the urgent need for cybersecurity awareness and training initiatives within South Africa, given the escalating Internet penetration across the continent, which has heightened susceptibility to cybercrimes targeting women. Despite recognizing the intersection between GBV and technology, significant challenges persist in adequately addressing emerging forms of gender-based cybercrimes within the existing legal frameworks, both domestically and internationally.

To address these challenges and enhance South Africa's response to cybercrime and GBV, the study proposes a set of recommendations aimed at improving law enforcement competency, increasing resources, empowering women, eliminating cybercrime safe havens, implementing policies, raising awareness, leveraging technology, and reforming social media platforms. These recommendations emphasize the importance of international cooperation and legal reforms to combat the multifaceted nature of gender-based cybercrimes effectively.

In conclusion, proactive measures informed by interdisciplinary collaboration, technological advancements, and policy reforms are essential for enhancing South Africa's response to cybercrime forms of GBV. By prioritizing the protection of vulnerable populations, fostering gender equality, and promoting responsible online behaviour, stakeholders within South Africa can collectively contribute to creating a safer and more inclusive cyberspace for all.

BIBLIOGRAPHY

Articles

Almenar R 'Cyber violence against women and girls: GBV in the digital age and future challenges as a consequence of Covid-19' (2021) 3(1) Trento Student Law Review 167-230.

Akdemir, N., Sungur, B., and Basaranel, B.U. (2020) Examining the Challenges of Policing Economic Cybercrime in the UK. Guven. Bilim.Derg. International Security Congress Special Issue,pp. 113-134

Anderson R and Baton C et al.. 'Measuring the changing cost of cybercrime' (2019) Presentedat: The 2019 Workshop on the Economics of Information Security, Boston US.

Agarwal N and Dr Kasuhik N 'Cybercrimes against women' (2014) 4(1) Global JournalResearch in management 37-49.

Bawa, N 'The regulation of the Interception of Communications and provision of Communication relation information Act' www.thornton.co.za (accessed 14 June 2023), 308.

Bossler, A., T.J. Holt, C. Cross, & G.W. Burruss (2019) Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness. Security Journal. DOI: 10.1057/s41284-019-00187-5.

Boukemidja N B 'Cybercimes against women : Qualification and means' (2018) 1(3)

Broadhurst, R. 2006. 'Developments in the Global Law Enforcement of Cyber-crime, Policing: An International Journal of Police Strategies & Management' 409.

Cassim F 'Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study' (2009) 12(4) Portchestroom Electronic Law journal available at https://www.scielo.org.za/scielo.php?script+sci_arttext&pid=S1727-37812009000400004 accessed on 24 June 2023.

Choi, K.S (2015) Cybercriminology and digital investigation. El Paso: LFB Scholarly Publishing.

Cronje, F. Snail, S. Olivier, A and Jordaan, J. 2022. The Cybercrime Act—What you need to

know .

Cross, C. (2019) Online fraud. Online Available from https://eprints.qut.edu.au/127162/

Dodge C, Burruss G (2019) Policing cybercrime. In: Leukfeldt R, Holt TJ (eds) The Human Factor of Cybercrime. Oxfordshire: Routledge.

Du Toit, P.G. (2023) "The search warrant provisions of the cybercrimes act and their relationship with the Criminal Procedure Act," Obiter, 43(4). Available at: https://doi.org/10.17159/obiter.v43i4.13191.

Essof S 'South Africa: Violence against women and information communication technologies' (2009) Association for Progressive Communications.

Eghtesadi M and Florea A 'Facebook , Instagram, Reddit and TikTok : a proposal for health authorities to integrate popular social media platforms in contingency planning amid a global pandemic outbreak' (2020) Can J Public Health 111 , 389-391.

Francis Cronje, Sizwe Snail, Anthony Olivier and Jason Jordaan, The Cybercrime Act—What you need to know (2022) at 3–4.

Goldsworthy, T., Crowley, J., & Raj, M. 2015. The conversation. Available from: http://theconversation.com/revenge-porn-is-just-one-part-of-a-changingpicture- of-harassment-43703 (Accessed 18 April 2022).

Grobler, M , Van Vuuren, J. Zaaiman, J. 2013 in" Preparing South Africa for Cybercrime and cyber defines" Systematics,cybermetics and informatics

Harshita, P (2021) '"Online violence against women is an overt expression of the gender discrimination and inequality that exists offline. Online, it becomes amplified."' https://www.thelawlegato.com/post/gender-based-cybercrime

Hinson L, Mueller J, O'Brien-Milne L, Wandera N 'Technology-facilitated GBV: What is it, and how do we measure it?' (2018) Washington D.C., International Center for Research on Women.

Human Rights Watch 'Submission by Human Rights Watch to the United Nations Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of

information and communication technologies for criminal purposes' 28th April 2022 available at https://www.hrw.org/news/2020/04/28/submission-human-rights-watch-united-nations-ad- hoc-comittee-elaborate accessed on 28 June 2023.

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Computer Law & Security Review, 27(1), 61–67. https://doi.org/10.1016/j.clsr.2010.11.001

Jansen van Vuuren, J, Grobler, M and Zaaiman, J. 2012. The influence of cyber security levels of South African citizens on national security. Proceedings of the 7th International Conference on Information Warfare and Security, Center for Information Assurance and Cybersecurity University of Washington, Seattle, USA, 22-23 March 2012

Kaur P and Vardhan R 'Cyber violence against women and girls (CVAWG) : Preparedness of cyber units in police stations in United States of America and women police stations in India (2020) (14) Intellectual Quest.

Kritzinger E , Bada M and Nurse JR-C 'A study into the cybersecurity awareness initiative for school learners in South Africa and the UK' (2017) Information Security Education for a Global Digital Society

Lucks, B. D. 2004. 'Cyberstalking: Identifying and examining electronic crime in cyberspace', Alliant International University, 2 (23).

Mabunda, S. M. 2021. The South African legislative response to cybercrime

Muncie, J., Talbot, D. & Walters, R. 2010. Crime: Local and Global. UK: Willan Publishing

Murali, S. (n.d.). KPMG INTERNATIONAL Issues Monitor Cyber Crime – A Growing Challenge for Governments Volume Eight. (PDF) KPMG INTERNATIONAL Issues Monitor Cyber Crime – a Growing Challenge for Governments Volume Eight | Sowmya Murali - Academia.edu.
https://www.academia.edu/5246982/KPMG_INTERNATIONAL_Issues_Monitor_Cyber_Crime_A_Growing_Challenge_for_Governments_Volume_Eight

Moyo, A. (2023) Police given power to intercept cellular communications, ITWeb. Available at: https://www.itweb.co.za/content/KA3Ww7dzBBkqrydZ (Accessed: 14 June 2023).

Nurse JR (2019) Cybercrime and you: how criminals attack and the human factors that they seek to exploit. In: Attrill-Smith A, Fullwood C, Keep M, et al. (eds) *The Oxford Handbook of Cyberpsychology*. Oxford: Oxford University Press.

Orji, U. J. (2014) Examining Missing Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection. Computer Law Review International, vol. 5, p. 132

Pashang S , Khanlou N and Clarke J 'The mental health impact of cyber sexual violence on youth identity' (2018) (17) International Journal of Mental Health and Addiciton.

Poland, B. 2020. Gendered Harassment, Abuse, and Violence Online. In: *Gender Violence, 3rd Edition: Interdisciplinary Perspectives*. New York University Press, 157-173.

Polity 'SAPS need resources and skills to fight cybercrime' 26th May 2023 available at https://m.polity.org.za/article/saps-need-resources-and-skills-to-fight-cybercrime-2023-05-26, accessed on 27 June 2023.

Poulpunitha, P. Manimekalai, K and Veeramani, P. 2020. 'Strategies to prevent and control cybercrime against women and girls'. 9(3) *International Journal of Innovative Technology and Exploring Engineering*.

Pukhraj Agarwal M 'Cyber Crime: Women combatting with the negative effects of technology in the era of globalization' (2020) 4(7) International Journal of Management and Humanities 23.

Reitano T, Oerting T and Hunter M 'Innovations in international cooperation to counter cybercrime: The joint cybercrime action taskforce (J-CAT)' (2015) 2(2) The European Review of Organized Crime 142-154.

Roberts, L. 2008. Cyber-Victimisation in Australia: Extent, Impact on Individuals and Responses. Briefing Paper No.6. Conducted by the Tasmanian Institute of Law Enforcement Studies.

Rhodes, L. M. 2012 'human trafficking as cybercrime' 2012 *AGORA International Journal of Administration Sciences* 25-26, available at https://univagora.ro/jour/index.php/ajas/article/view/2992/1138. Accessed on the 23 June 2023.

Snail S (2009) “Cybercrime in South Africa – Hacking, Cracking and Other Unlawful Online Activities” 138 Journal of Information, Law & Technology 1-13.

Sagwadi Mmahlatse Mabunda (2021) “THE SOUTH AFRICAN LEGISLATIVE RESPONSE TO CYBERCRIME”

Security for Sustainable Technology Innovation and Economic Growth . Technology and Exploring Engineering. European Journal of Social Sciences 35-36.

Snail ka Mtuze, S., Musoni, M. 2023. An overview of cybercrime law in South Africa. *Int. Cybersecur. Law Rev*. https://doi.org/10.1365/s43439-023-00089-8

Stander A, Dunnet A & Rizzo J (2009) ‘“A Survey of Computer Crime in South Africa’” Proceedings of ISSA 2009 Conference 217-226

Soulcity.org.za. 2021. [online] Available at: <https://www.soulcity.org.za/campaigns/gbv/resources/understanding-gender-policy-and-gender-based-violence-in-south-africa-a-literature-review> [Accessed 17 September 2023].

Sundani N , Mangaka A.C and Mamokhere J ‘Social media as a campaign tool against online GBV in South Africa (2022) Science Rise (5) 30-41.

Tatarinova L F and Karimzhan et al .. ‘Criminological analysis of determinants of cybercrime technologies’ (2016) 11(5) IEJME-Mathematics Edition 1131.

United Nations Entity for Gender Equality and the Empowerment of Women.

Wall, D. S. 2005. The Internet as a Conduit for Criminal Activity. In: Pattavina, A. (Ed.), Information technology and the Criminal Justice System. Chicago:Sage Publications.

Warner E and Miedema X et al.. (2013) ‘Why do some men use violence against women and how can we prevent it? Multi-country study on men and violence in Asia and the Pacific’

Welsh, A. & Lavoie, J.A.A. 2012. Risky eBusiness: An Examination of Risk-taking, Online Disclosiveness, and Cyberstalking Victimization. Cyberpsychology: Journal of Psychosocial Research on Cyberspace

Yeop Paek S and Nalla M K et al.. ‘The perceived importance of cybercrime control among police officers: Implications for combatting industrial espionage’ (2021) 13(8) Industrial

Case Law

AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services 2020 (1)SA 90 (GP)

Bernstein and Others v Bester and Others NN0 1996 (2) SA 751 (CC)

Financial Mail (Pty) Ltd and Others v Sage Holdings Limited and Another 1993 (2) SA 451 (A).

Goqwana v Minister of Safety and Security 2016 (1) SACR 384 (SCA).

High Court of South Africa in Johannesburg, Case No 23897/17

Le Roux v Dey (2011) 3 SA 274 (CC)

Manyi v Dhlamini 2018 ZAGPPHC

Minister of Police v AmaBhungane Centre for Investigative Journalism NPC [2021] ZACC 3; 2021 (4) BCLR 349 (CC);

*Minister for Safety and Security v Van der Merwe*2010 (1) SACR 470 (C)

Mgoqi v S [2020] ZAECGHC

Myeni v S [2018] ZAECGHC

Mogale v Minister of Safety and Security 2016 (2) SACR

National Coalition for Gay and Lesbian Equality and Another v Minster of Justice and Others 1999 (1) SA 6 (CC)

Prinsloo v S Case number (613/2013) ZASCA

Okundu v S [2016] ZAECGHC

Oosthuizen v Magistrate, Hermanus 2021 (1) SACR 278 (WCC

Salzmann v S Case number (755/2018) ZASCA

South African National Editors Forum and Others v Black Land First and Others,

(23897/17) [2017] ZAGPJHC 179 (7 July 2017)

T G v W C (3198/2019) [2020] ZAGPJHC

Thint (Pty) Ltd v NDPP, Zuma v NDPP 2008 (2) SACR 421 (CC)

Van Der Berg v Coopers and Lybrand Trust (Pty) Limited and others 2011 (3) SA 274 (CC).

Commissions of inquiry and government committees

Van der Wilk A, Council of Europe – Protecting Women and Girls from Violence in the Digital Age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women (2021) 26-27.

Department of Justice and Constitutional Development National Strategic Plan on GBV and femicide (2020) available at https://www.justice.gov.za/vg/gbv/nsp-gbvf-final-doc-04-05.pdf accessed on 28 June 2023.

UN Women Safe Digital Spaces : Protection of Women and Girls from Technological Violence (2020) available at https://africa.unwomen.org/sites/default/files/Field%20office%20Africa/Attachments/Publica

tions/2020/Backgroundpaper.Webpdf accessed on 28 June 2023.

Corporate bodies as authors – companies ,organisations , institutions

AU Convention on Cybersecurity and Personal Data Protection.

Beijing Declaration and Platform for Action of 1995

Human Rights Council, 2016

Protocol to the African Charter on Human and Peoples Rights on the Rights of women in Africa.

United Nations Office on Drugs and Crime A Training Handbook for Criminal Justice Practioners on Cyberviolence against women and Girls (VAWG) (2022) 46-60.

UN General Assembly, 2006

SADC Protocol on Gender and Development (2016).

Thesis

Basson , L Cyberviolence against Women and Girls : Taking a step forward for Female inclusion in the Digital Era (LLM thesis , Ca 'Foscari University of Venice , 2004).

Chanana, P. 2017. The role of UN women towards the development and advancement of women in Southern Africa: a critical comparison between South Africa and Zimbabwe. University of Pretoria.

Malin, J Gender-Based Online Hate Speech Against Women (Master Thesis in Legal Science, Orebro University , 2022) 23-24.

Griffiths J.L Cyber-security as an emerging challenge to South African national security (Mini dissertation Masters, University of Pretoria, 2017).

Gervasius, N 'Understanding Online GBV' (2021) Centre for Human Rights, University of Pretoria.

Website Documents

All reports on the country visits of the UN Special Rapporteur on violence against women and girls, its causes and consequences are available at: www.ohchr.org/en/special-procedures/sr-violence-against-women/country-visits

Botnets as a vehicle for Online Crime,2005, available at: www.cert.org/archive/pdf/Botnets.pdf;Barford/Yegneswaran,An inside Look at Botnets, available at:http://pages.cs.wisc.edu/~pb/botnets final.pdf; Jones, Botnets: Detection and Mitigation.

Casey, Digital Evidence and Computer Crime,2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime,2005, Cybex, available at: www.cybex.es/agis2005/elegir idioma pdf.htm.

College of Policing (2020) Investigation Process. Retrieved from: https://www.app.college.police.uk/app-content/investigations/investigation-process (Accessed 1 September 2023).

Council of Europe Portal 'Cyberviolence against women' (2023) available at https://www.coe.int/en/web/cybe men rviolence/cyberviolence-against-women accessed on 28 June 2023.

Council of Europe, 2022. *The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform* Online: OHCHR

Fighting Cyber Crime and Terrorism: The Role of Technology, presentation at the Stanford Conference, December 1999. The Transnational Dimension of CyberCrime and Terrorism, 2001 available at http://media.hoover.org/documnets/0817999825 1.pdf.

Human Rights Watch 'Submission by Human Rights Watch to the United Nations Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes' 28 th April 2022 available at https://www.hrw.org/news/2020/04/28/submission-human-rights-watch-united-nations-ad- hoc-comittee-elaborate accessed on 28 June 2023.

ICRW | PASSION. PROOF. POWER. 2022. Technology-Facilitated GBV: What is it, and How do we measure it? [online] Available at: https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/ [Accessed 19 April 2022].

IPU study reveals widespread sexism, harassment and violence against ... Available at: https://www.ipu.org/news/press-releases/2016-10/ipu-study-reveals-widespread-sexism-harassment-and-violence-against-women-mps (Accessed: 04 February 2024).

National Sovereignty is a fundamental principle in International Law. See Roth, State Sovereignity, International Legality and Moral Disagreement,2005, available at www.law.uga.edu/intl/roth.pdf.

Pambazuka.org. 2021. The Maputo Protocol: Evaluating women's rights | Pambazuka News. [online] Available at: https://www.pambazuka.org/gender-minorities/maputo-protocol-evaluating-women%E2%80%99s-rights [Accessed 20 February 2023].

Polity ‘SAPS need resources and skills to fight cybercrime’ 26 th May 2023 available at https://m.polity.org.za/article/saps-need-resources-and-skills-to-fight-cybercrime-2023-05-26, accessed on 27 June 2023.

The Parliament Magazine. 2022. ‘Gender-based cyberviolence: The new face of an old enemy’’. Available at: <https://www.theparliamentmagazine.eu/news/article/genderbased-cyberviolence-the-new-face-of-an-old-enemy> [Accessed 18 April 2022]

Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders’ United Nations 2000, available at http://bit.ly/2kjJFXN accessed on 26 May 2022.

UN Women *Safe Digital Spaces: Protection of Women and Girls from Technological Violence* (2020) available at https://africa.unwomen.org/sites/default/files/Field%20office%20Africa/Attachments/Publications/2020/Backgroundpaper.Webpdf accessed on 28 June 2023.

Women abused on Twitter every 30 seconds - new study (no date) *Amnesty International UK*. Available at: https://www.amnesty.org.uk/press-releases/women-abused-twitter-every-30-seconds-new-study (Accessed: 04 February 2024).

What is hate speech? United Nations. Available at: https://www.un.org/en/hate-speech/understanding-hate-speech/what-is-hate speech?gclid=Cj0KCQjw7aqkBhDPARIsAKGa0oJAI3HpfAy7vcWWfLDS3kRkbt3pfL6fGVNu37Pe3cKqF_cCOKb-GogaAiZ7EALw_wcB (Accessed: 15 June 2023).

Legislation

Constitution of the Republic of South Africa, Act 108 of 1996

Copyright Act 98 of 1978.

Cybercrimes Act 19 of 2020.

Films and Publications Act 65 of 1996

The Declaration acknowledges poverty as a challenge experienced by women, which includes issues such as early marriages, limited access to education, social and political discrimination, and exclusion. Governments were urged to eradicate disparities between women and men in accessing education and achieving educational outcomes across all levels and forms of education.

UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

Mr Suhail Jadwat (218006111)
School Of Law
Howard College

Dear Mr Suhail Jadwat,

Original application number: 00017306
Project title: A critical review of South Africa's Response to Cybercrime forms of Gender-Based Violence

Exemption from Ethics Review

In response to your application received on 19 May 2022 , your school has indicated that the protocol has been granted **EXEMPTION FROM ETHICS REVIEW.**

Any alteration/s to the exempted research protocol, e.g., Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through an amendment/modification prior to its implementation. The original exemption number must be cited.

For any changes that could result in potential risk, an ethics application including the proposed amendments must be submitted to the relevant UKZN Research Ethics Committee. The original exemption number must be cited.

In case you have further queries, please quote the above reference number.

PLEASE NOTE:
Research data should be securely stored in the discipline/department for a period of 5 years.

I take this opportunity of wishing you everything of the best with your study.

Yours sincerely,

[redacted]

Mr Matthew Blain Kimble
obo Academic Leader Research
School Of Law