MIDLANDS STATE UNIVERSITY

FACULTY OF SOCIAL SCIENCES

DEPARTMENT OF MEDIA AND SOCIETY STUDIES

Investigating the relevance of the introduction of the Cybercrime and Cybersecurity Bill, 2017 in Zimbabwe

By

Silas Deya (R144855T)

Supervisor: Professor N. A. Mhiripiri

A dissertation submitted to the Faculty of Social Sciences in partial fulfilment of the requirements for the Bachelor of Science Honours Degree in Media and Society Studies.

Gweru, Zimbabwe

June 2018

Declaration

I, Silas Deya (R144855T), hereby declare that this dissertation is my original work that has not been previously submitted to any other university. Equally, I declare that proper citations and acknowledgements in accordance with copyright law and ethical considerations have been strictly adhered to in the compilation of this research.

Student's Signature ______________________________

Date ____

Certification of supervision

I hereby certify that I personally supervised this dissertation in accordance with the departmental regulations and the university's general regulations. On that basis, I confirm that the dissertation is examinable.

Title: Investigating the relevance of the introduction of the Cybercrime and Cybersecurity Bill, 2017 in Zimbabwe

Name of Supervisor: Professor N. A. Mhiripiri

Signature ______________________________

Date ___________________________________

Acknowledgements

My sincere gratitude goes to my supervisor, Professor Nhamo Anthony Mhiripiri who helped me throughout my project and his constructive ideas shaped this research. I cannot thank him enough for the knowledge he shared with me, patience, guidance and support he provided.

I would also like to extend my gratitude to all the lecturers in the Media and Society Studies Department, not forgetting my friend Varaidzo Nemaramba for the advice and support which kept me going in times that I felt weary.

To my mother, Florence Tomu, thank you for unconditional love, material support and guidance, without which I would not have come this far. My appreciation goes beyond what words can express.

Dedication

I dedicate this research to God Almighty my creator, my strong pillar, my source of inspiration, wisdom, knowledge and understanding. He has been the source of my strength throughout and on his wings only have I soared.

I also dedicate this work to my late father Silas Deya (Snr), mother Florence Tomu who has encouraged me all the way and whose encouragement has made sure that I give all it takes to finish that which I had started. To my siblings Tendayi, Tineyi, Fungai, Wellington and Simbarashe who have been affected in every way possible by this quest.

Abstract

The study investigates whether the Cybercrime and Cybersecurity Bill of 2017, is needed in Zimbabwe. The bill is yet to be enacted into law and it is still waiting for the President's signature. The study seeks to find out the different contestations surrounding the bill and to highlight some major concerns in as far as cybercrimes and cybersecurity are concerned in Zimbabwe. Law enforcing agents, internet users and news articles were used as the research population in a bid to hear the views of some sections of the society. Owing to the qualitative nature of the research, the researcher employs non-probability sampling, specifically purposive sampling to single out representative samples of the study. Data collected is analysed using the Critical Discourse Analysis and it is presented thematically. The findings reveal that the bill is very relevant and is urgently needed in Zimbabwe but there has to be amendments to be made first to make sure that the bill does not contradict with the constitution in terms of freedom of expression and the right to privacy.

Contents

CHAPTER ONE: INTRODUCTION TO THE STUDY

1.0 Introduction

As the world is fast becoming one and new information communication technologies (ICTs) are being invented, almost on a daily basis, the extent of cybercrimes within countries and the world at large is reaching an immense proportion (Malby et. al, 2013).

Cybercrimes can be defined as offences that are committed against individuals or groups of individuals through electronic means and telecommunication networks like internet chat rooms, emails, mobile phones by way of text messages (Maat, 2009). Like any other crimes, cybercrimes tend to pose dangers to national security, individuals and can as well be a threat to financial security if not well addressed.

Halder & Jaishankar (2011:12) further defines cybercrime as:

> Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

The duo further states that issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

The main purpose of this research was to investigate the relevance of Zimbabwe’s Cybercrime and Cybersecurity Bill which is still awaiting the country’s President’s signature in order to become an Act; hence a binding law or legal instrument. The bill was drafted by the Ministry of Information and Communication Technologies (ICTs), Postal and Courier Services now called the Ministry of ICTs and Cybersecurity and it addresses current legislation shortcomings.

This study also had the task to examine the feasibility of such a law in Zimbabwe and also examine if the bill tally with the Constitution of Zimbabwe Amendment (No. 20) Act 2013 in terms of freedom of expression as well as ensuring user protection of privacy.

Then bill under study started to be drafted in June 2013 and was called the Computer Crime and Cybercrime bill and an initial draft was surfaced in August 2016. On June 9, 2017, the then Ministry of Information Communication Technology, Postal and Courier Services presented a third draft of the bill and had slightly changed the name to Cybercrime and Cybersecurity bill, 2017. The changes were made as an attempt to bring it within the more universally acceptable clauses that are in sync with national, regional and international best practices.

1.1 Background of study

Citizens' participation in the cyberspace mainly online social media platforms such as twitter, Facebook, Instagram among a plethora of other examples has been dubbed as a major threat to national and individual security in many countries worldwide since its early days (Belk and Noyes, 2012).

Studies concur that cybercrime is a new challenge that has been added to a host of other challenges that are already bedevilling the African continent with most countries having been caught unprepared in terms of awareness, laws, technical expertise and technical resources (Akuta et al, 2011; Odumesi, 2006; Herselman and Warren, 2004). Against this background, it is of paramount importance to have collective efforts in Africa aimed at promoting cyber security in the continent.

The dissident use of social media or the internet to oppose the government in Zimbabwe has increased in the last few years, beginning with Baba Jukwa on Facebook (Mutetwa, 2015) and culminating with #ThisFlag. These and other global trends on cybercrime have prompted Chitauro (2015) to advocate that laws to curb cybercrime are vital to the nation of Zimbabwe.

In this regard, several measures have been taken by the country to make sure they control and monitor the cyberspace and terminate cybercrime.

Over the years, the government of Zimbabwe has made great strides in an attempt to deal with the issue of computer and cybercrimes. In 2002, the Postal and Telecommunications Act was enacted which was meant to guide jealously the use postal and telecommunications industry.

In 2007, the Interception of Communications Act was passed making sure that all telephone lines are registered. Before a telecommunication service provider enters into a contract with any person for the provision of a telecommunication service to that person, it must obtain the person's full name, residential address, business address and postal address and his or her identity number contained in his or her identity document.

In 2013, the then Ministry of ICTs, Postal and Courier Services started to draft the Cybercrime and Cybersecurity Bill. It was an attempt to keep up with global trends, as it is now necessary for all countries to come up with laws that classify and deal specifically with cybercrimes for, without dedicated statutes, there will be no legal mechanisms on which to prosecute the cybercriminals (Majome, 2017).

The introduction of the bill provides that it is intended for an act to criminalise offences against computers and network related crime, to consolidate the criminal law on computer crime and network crime; to provide for investigation and collection of evidence for computer and network related crime; to provide for the admission of electronic evidence for such offences and to provide for matters connected with or incidental to the foregoing.

In 2017, a whole ministry was setup to mitigate cybercrime called Ministry of Cyber Security, Threat Detection and Mitigation which was later merged with the Ministry of ICTs, Postal and Courier Services to make Ministry of ICTs and Cyber Security by President Emmerson Mnangagwa.

The complexity of crimes committed through and against computers requires special attention, but further more speed and spread of such crimes presents difficulties, which has caused many governments to abrogate rights and freedoms in the pursuit of security and safety. Computers and cyber spaces have become platforms for expression, protesting, collective voice, which used to take places in open markets and streets. The places to protest are now online, with emerging trends of virtual sit-ins, cyber activists (MISA Zimbabwe, 2016).

Furthermore, Hansen and Nissenbaum (2009) discovered that some regimes, for example, China have gone to the extent of banning the use of social technologies citing their destabilising nature as witnessed by most uprisings of the recent past. China in the recent past has been seeking to block the use of social technologies by its citizens citing that they are a threat to the stability of society and politics at large.

It is against this background that this study sought to investigate whether Zimbabwe was in a position to adopt such a law and assessing whether it was going to be possible to implement such a legislation.

1.2 Statement of the problem

Despite the development brought by the use of the internet, it has emerged cybercrimes. There is a tremendous growth of cybercrimes in the country whereby consumers online are at stake as some internet users are now exploiting the cyberspace in committing crimes like cyber bullying, cyber terrorism, defaming others as well as spreading false news and rumours among others. This work critically reviews the legal framework on cyber laws in Zimbabwe and sees whether the same has addressed cybercrimes adequately. It investigates the relevance of the newly proposed Cybercrime and Cybersecurity bill.

1.3 Research Objectives

The study is anchored on three specific objectives, which are:

- Exploring the relevance of the Cybercrime and Cybersecurity bill in Zimbabwe.
- Examining the effectiveness of the current legislation in addressing issues related to cybercrime.
- Analysing the feasibility of the bill in Zimbabwe and its impact on freedom of expression as enshrined in the Constitution of Zimbabwe.

1.4. Main Research Question

- What is the relevance of the Cybercrime and Cybersecurity Bill in Zimbabwe?

1.4.1 Sub Research Questions

- How is the current legislation addressing issues related to cybercrime?

- How will the bill affect freedom of expression as enshrined in the Zimbabwean constitution if passed into am act?

1.5 Justification of the study

It is the study's duty to enrich the existing body of knowledge about cybercrimes in Zimbabwe. The findings obtained through this study benefitted the media fraternity, the public at large and the policymakers by letting them know what cybercrimes are, the challenges and the remedies pertinent to cybercrimes, the legal framework there to and the need to adopt or do away with the bill under study.

The study also observes and recommends what should be done based on best lessons from other jurisdictions with a suitable legal framework to combat cybercrimes at the same time upholding the free expression and access to information on the internet. Cybercrime in the country has been under researched and the bill under study is currently new hence, there has not been much research about it.

1.6 Scope of the study

Delimitations are those elements which limit the study's scope and also define boundaries of the same (Simon, 2011). This study therefore, seeks to investigate whether Zimbabwe is ready for such an act or not, paying particular attention to its impact on the freedom of expression and freedom of the media. It is against this background that the study focuses only on how the bill will affect the media industry and the public at large if passed into an act.

1.7 Limitations

Limitations are influences that the researcher cannot control. Though the study focused on the relevance of the bill in Zimbabwe, the researcher could not afford to get responses from all corners of the country hence had to get opinions from people who were available at the time the research was carried which led to the generalisability of the findings. This same was done to newspaper articles which were used in the study. The researcher intended to interview Members of Parliament in the Parliamentary Portfolio Committee on Media, ICTs and Cybersecurity and he could not get hold of them as the research was conducted towards elections, most of them were busy campaigning and had no time to entertain the researcher. This affected the findings as there was need for the researcher to also hear the views of these policy makers.

1.8 Assumptions

- The Cybercrime and Cybersecurity bill is very vital in Zimbabwe due to the rise in the use of social media in the country hence need to protect citizens.
- The Cybercrime and Cybersecurity bill have a negative impact on the freedom of expression in Zimbabwe.
- The bill might face problems in trying to persecute perpetrators of cybercrime who reside abroad.
- The legislation was meant to silence opposition political parties who had taken social media by storm as they were denied enough coverage by the government controlled mass media.

1.9 Structure of the study

The study is divided into six chapters. Chapter one outlines the introduction to the study, while chapter two consists of literature review and theoretical framework. Chapter three outlines the research methods and methodology. Chapter four focuses on the political economy of the Ministry of ICTs and Cyber Security. Chapter five outlines the research findings of the study and chapter six outlines recommendations and concludes the study.

1.10 Conclusion

This chapter provided the foundation and an insight of the study. It encompassed the introduction, background of the study, statement of the problem, research objectives and questions, justification, scope, limitations, assumptions and structure of the study.

CHAPTER TWO: LITERATURE REVIEW AND THEORETICAL FRAMEWORK

2.0 Introduction

This chapter introduces the literature review and theoretical framework for this study. The chapter is very vital for the study because it enabled the researcher to come out with themes and theories, which are relevant for the study.

2.1 Literature Review

Literature review can be discussed as the discussion of published information that relates to a particular subject at a certain period. Aveyard (2010) denotes that a literature review is comprehensive study and literature that addresses a specific topic.

2.1.1 Digital public sphere monitoring challenges

The concept of public sphere and media regulation have dominated much of the recent literature in media studies. Different scholars have tried to explore the connection between the public's access to the public sphere (i.e. the media) and regulation (Mhiripiri and Chari, 2017; Mutsvairo, 2016; Kasoma, 2013; Chari, 2013; Chibuwe, 2012; Packard 2010). Many researchers are concerned with how regulation stifles freedom of expression in the traditional media but these scholars moved a step to analyze the digital public sphere. Mhiripiri and Chari (2017) highlighted that most current books on media law and ethics were simply crafted with traditional media in mind, meaning that there is a shortage of literature in relation to law and ethics with regards to the new media including social media and mobile communication.

Political and commercial interests take precedence in the constructing of media policies, as users are not perceived as a public but as consumers (Chibuwe, 2012). He further outlines that the issue of media regulation and the digital public sphere is relevant across the world, even though the digital public sphere in most of the third World countries, Zimbabwe included, is not as developed as it is in Europe, largely because of political, economic and technological challenges. This assertion concurs with Chari (2013:379) when he notes that:

> Online publications have become critical sites for the expression of views alternative to those of the state. This is true in Zimbabwe as in many

> developing states where the mainstream media operate under onerous legislative frameworks.

Ronning as cited by Chibuwe (2012) argues that the internet has qualities that make it a very advanced tool for surveillance and must be seen in relation to the increasing number of legal provisions and technical systems of surveillance and interceptions of communications now used. In this regard, issues of security, morality, religion, copyright and outright dictatorship facilitates the regulation of the cyberspace. Mutsvairo (2016) further supports this assertion as he asserts that digital technologies have in a big way disrupted the manner in which media are consumed worldwide as they have posed serious threats to legacy media. He notes, "digital media have … often served as channels for hate speech, intolerance and increased the disempowerment of those citizens who lack access or the ability to use these platforms to full effect" (Mutsvairo, 2016: v).

In addition, Packard (2010) as cited by Mhiripiri and Chari (2017) argued that it is high time people stop thinking about media law as though it were the exclusive domain of traditional media organisations as the global shift to digital media has precipitated a shift in information control. He further argues that almost everyone has become media producer it is indeed a noble idea that everyone should know something about media laws to protect their own rights and to avoid violating the rights of others.

Old laws cannot keep up with the advancing technologies and law breaches by citizen journalists hence there is need for policy makers to constantly upgrade laws to safeguard their people. Mhiripiri and Chari (2017: xx) argue that:

> The digital explosion has spawned new journalistic practices, which have rendered the old laws and ethics redundant, thus rendering media regulatory authorities as sitting ducks as they watch laws and ethics being flouted by bloggers and citizen journalists who seemingly have become law unto themselves.

The above argument is also in tandem with Chibuwe (2012:625) when he argues, "Online democracy is tricky, as it must be reconciled with many misuses of the internet, such as its successful use by terrorists and hate groups operating in the cyberspace".

Many governments, especially in Africa and in Asian countries such as China, have tried to block diverse and open communication, but social media have disrupted these restrictive practices, (Chatora, 2012). However, Yanshuo (2017) opposes this argument as he highlighted that China's cyber law tend to guard against its citizens as well as protecting them from unscrupulous individuals who misuse the cyberspace. The Cybersecurity law of China advocates that internet users be not allowed to leak, change or damage personal information to others without the consent of the people involved which is a great deal for the internet users in China (Yanshuo, 2017). Cyberspace users are also obliged to take measures to ensure that the personal information they collect is secure.

The major advantage of using social media for communicating is the near absence of traditional methods of regulation (Squires, 2002). A government can attempt to restrict the content of social media, but traditional censorship cannot keep up with ever-changing web pages. However, Mhiripiri and Chari (2017) tends to disagree with this assertion as they argued that ordinary members of the public and professional communicators also need to be well equipped with the basic ethical standards associated with communicating online as well as respective regulatory and policy environments in order for them to cope with minimal problems as national or global citizens.

Samuelson (1998) highlighted five key policy challenges associated with monitoring the cyberspace. The challenges include whether the laws can apply or adapt existing laws and policies to the regulation of internet activities, or whether the new laws policies are needed to regulate internet conduct. She adds that how to formulate a reasonable and proportional response when new regulation is needed, how to craft laws that will be flexible enough to adapt to rapidly changing circumstances. Also, how to preserve fundamental human values in the face of economic or technological pressures tending to undermine them and how to coordinate with other nations in internet law and policy making so that there is a consistent legal environment on a global basis.

It is against this background that this study seeks to examine the relevance of the Cybercrime and Cybersecurity Bill in Zimbabwe, which is still waiting for the President's signature for it to become an act, focusing on whether if the bill will manage to monitor the cyberspace if passed into an act and its implications on the freedom of expression.

2.1.2 Cyber Security in Zimbabwe

Zimbabwe, like all other countries, has not been spared by the scourge of cyber space threats prompting Madondo (2017) to argue that the problem in Zimbabwe is that there is no cyber security in place. United Nations Institute for Disarmament Research (UNIDIR) (2013) as cited by Madondo (2017) highlighted that Zimbabwe launched the Information Technology Governance and Cyber Security Institute of Sub-Sahara in early 2012 with its mandate to increase information exchange, promote research and reporting of cyber threats and hold periodic ICT security symposiums.

Zimbabwe is ill prepared for cyber security and hence vulnerable to cyber terrorism as 140 cases of cybercrimes were reported between 2011 and 2015 (Madondo, 2017). He further notes that Zimbabwe has witnessed significant growth of the internet, with statistics showing a penetration rate of 50% in 2016, according to the Postal & Telecommunications Regulatory Authority of Zimbabwe (POTRAZ, 2017). As at 30 June 2017, the total number of internet subscriptions was 6,668,155 (POTRAZ, 2017). The same report highlighted that Zimbabwe had 12,878,926 mobile phone subscribers. In 2015, Facebook was the most popular platform in Zimbabwe and twitter was slowly gaining momentum (MISA-Zimbabwe, 2015). This saw mobile internet data usage up by 19%, whilst national mobile voice traffic declined by 15% (POTRAZ, 2017). This means internet use is growing fast in Zimbabwe.

Zimbabwe has suffered a number of cyber security breaches on various institutions but mostly in government departments. According to the Reserve Bank of Zimbabwe (RBZ) (2015), cybercrime is listed as one of the crimes contributing to the US$1, 8 billion estimated illicit proceeds generated from criminal activity annually in Zimbabwe. Of the 140 cases of cybercrimes reported, they included; Phishing (20); Credit Card Fraud (13); Identity Theft (10); Unauthorized Access (24); Hacking (72); and Telecommunications Piracy (1). These statistics are evidence of Zimbabwe's vulnerability to computer and cybercrimes and thus the pressing need for a legal framework to combat these crimes before they become pervasive (MISA-Zimbabwe & Digital Society Zimbabwe, 2016). Further, approximately 37 government related sites were hacked between 2013 and 2016.

According to Njanjamangezi (2014), Munyaradzi Gwatidzo the Chief Executive Officer of Astro mobile asserts that more than 90% of organisations in Zimbabwe are exposed to cyber security risks. This has been as a result of many factors chief among them being the poor economic performance being experienced in the country prompting organisations to fail to acquire equipment and training that can cushion themselves against these risks.

Furthermore, Zimbabwe - just like most global nations - lacks statutory instruments that can be used to protect organisations from cyber security risks (MISA-Zimbabwe & Digital Society Zimbabwe, 2016). They further argue that the legislation in Zimbabwe have not progressed as fast as the evolution of technology with regards to the regulation of cyberspace that balances the right to freedom of expression and access to information and the protection of citizen's rights. This entails that governments are entirely reliant on the technical implementations in order to cushion themselves from the prevalent cyber security risks. With this predicament, it is crucial for Zimbabwe to develop strong legal instruments which will make the cyberspace a safe haven for its users.

According to Ncube (2014), the government of Zimbabwe is formulating laws to regulate the activities on social media in order to protect its citizens and the state from cybercrimes. He highlighted that this has to be done in order to remedy the outdated cyber laws, as is the case for many African countries. When enacted, the laws will play the role of regulating social technologies content as well as protecting the privacy of the public from hackers. He further states that the government acknowledges the dynamism of technology and hence have devoted to be on their toes in the regulation process.

This has been reflected by the failure of the government to adequately deal with the Facebook case of Baba Jukwa and ended up offering US$300 000.00 reward to anyone who was able to expose Baba Jukwa (Sabao and Chingwaramuse, 2017).

Thus, it is this study's aim to explore the neediness of a legislation that governs cyber security and terminate cyberspace in the era of new ICTs in protection of privacy and online users as well media responses on the bill.

2.1.3 Internet governance as a tool to stifle human rights

Recent studies on internet governance has agreed that internet governance is a direct tool used by governments to choke human rights, though the regimes pretend to be protecting the public (Yanshuo, 2017; Zimbabwe Democracy Institute & Media Centre (ZDI & MC), 2017, 2018; Collaboration on International ICT Policy for East and Southern Africa (CIPESA), 2016). Most countries' constitutions guarantee freedom of the media, internet freedom included but some laws being enacted in these countries tend to contradict with the constitution. ZDI & MC (2018: 3) noted, "The new constitution of Zimbabwe extensively guarantees internet freedoms which the cybercrime bill tends to stifle". The constitution recognises the need to uphold democracy, good, transparent and accountable governance and the rule of law. It also reaffirms the people's commitment to upholding and defending fundamental human rights and freedoms. Thus, ZDI & MC (2018) argues that the bill is quiet on safeguarding citizen's liberties and enhancing accountability in the process of eradicating cybercrimes. "… powers behind this bill were solely preoccupied with their desire to monitor and regulate citizen's use of the internet and thwart their desire to harness opportunities to claim all other liberties (ZDI & MC, 2018:4).

Zimbabwe currently suffers the conspiracies of an authoritarian regime that fears freeing the social media, private media and the internet in general due to the belief that in doing so it will prevent possible public scrutiny, transparency, criticism and exposure of its maladministration (ZDI & MC, 2017).

Furthermore, CIPESA (2016) highlighted that the government of Zimbabwe is working tirelessly on a raft of laws to regulate internet use with touted objective of upholding protection of user's privacy as well as curbing cybercrimes, however the measures are likely to strengthen the government's arsenal for violating citizen's internet freedom.

Internet freedoms as being one of people's rights should be upheld all the time, hence the study seeks to outline the significance of the bill under study in Zimbabwe as far as promotion of human rights is concerned.

2.2 Theoretical Framework

The term theoretical framework according to LeCompte and Preissle (1993) is a collection of interrelated concepts that can be used to direct research with the purpose of predicting and explaining the results of the study.

2.2.1 Democratic Participant Media Theory

The study is guided by the democratic participant theory of the media. The theory purports that media and communication systems play an important role in upholding democracy and this role should somehow guide the work of media organisations and the public policies that shape the structures and conditions of the media system (Karppinen, 2013). In the context of this study, the researcher examine the feasibility of internet regulation legislation in relation to issues of democracy in Zimbabwe.

The theory advocates for the right to communicate to all citizens either as individuals or groups and highlight that the media should always serve the needs of all people. McQuail (1983:97) highlights that:

> Individual citizens and minority groups have the right of access to media – the right to communicate – and the right to be served by media according to their own determination of need; the organisation and content of media should not be centralised to political of state bureaucratic control.

In relation to this study, democratic participant theory is employed to examine the extent to which Zimbabwean citizens uses the internet to democratically air their views.

In addition, the theory emphasises that the prevailing democratic, commercial and professional hegemony in media system should be done away with so as to make sure that there is an easy access to the media by allowing potential users and consumers (Wood, 1997). It clearly suggests that small-scale media enterprises should replace or co-exist with media conglomerate. It also suggests horizontal as against top-down communication. It brings to light its commitment to feedback in social political communication in order to attain completed communication circuit. The mass has become too important socially, it should not only be left in the hand of the professionals hence the theory has been described as the press equivalent of grassroots democracy. However, this is an approach which has given society a false political and economic value as the entire society is not considered in the decision-making process and the issue of democratically participating especially using the social media is one which has over the years created fears among many governments.

Moreover, Kapor (1993:53) notes that "life in the cyberspace seems to be shaping up exactly like Thomas Jefferson would have wanted: founded on the primacy of individual liberty and a commitment to pluralism, diversity and community". He further argues that on the other hand the negative interpretation of the relationship between the internet and the politics revolves around the risk carries the potential for misinformation and over information circulation in cyberspace giving way to passivity and manipulation of political opinions of its users.

The internet according to Thornton (2002) has caused an explosion of direct participatory democracy. Citizens from all works of life, encompassing those from middle income groups and lower income groups, people who live in areas distant from political power centres, those who previously had no direct access to political participation at the policy level, now can find a voice through the internet. Internet meets the people's demand for political information in a more convenient form, at a lower cost i.e. price, and time than in the traditional media and this has helped to improve citizens' participation in public affairs.

The democratizing potential of new media practices in relation to news and journalism have been argued by Hartley (2008, 2009), Bruns (2008) and McNair (2006) among others. McNair (2006:199) proposes that:

> In the era of cultural chaos, people have access to more information than ever before. If information is the pre-requisite of knowledge, and if knowledge is power, other things remaining equal, this trend corresponds to a power-shift from the traditionally information-rich elite to the no longer so information-poor mass.

Thus, internet in general can promote democracy. The basic logic is that cyberspace offers more opportunity for people to discuss and influence public affairs to make sure that public policies are fit for personal proper demand, which is an essential meaning of democracy hence the study used the democratic participant theory as its base to investigate the relevance of regulating the internet in the country.

2.2.2 Democratising the Public Sphere

The public sphere concept is still very hard to understand as it lacks a clear definition and surrounded by many contestations (Adolf and Wallner, 2005). The public sphere can be defined as the focal point of participatory approaches to democracy, it is an arena where the populace gathers to exchange opinions regarding public affairs, discuss, deliberate and eventually form public opinion (Mhiripiri and Mutsvairo, 2013). The public sphere can also be defined as a discursive space in which individuals and groups congregate to discuss matters of mutual interest and where possible to reach a common judgement (Hauser, 1998 as cited by Mhiripiri and Mutsvairo, 2013).

The concept of the public sphere was originally brought about by Habermas (1989) as his major concern was the coming together of citizens and the discussion of ideas often related to governance and democratic ideals (Javuru 2013:368). Keane (2004) as cited by Javuru (2013) defines the public sphere as a particular type of spatial relationship between two or more people, usually connected by a certain means of communication.

The rise of new media technologies has led to the rise of new digitised public sphere. Mhiripiri and Mutsvairo (2013:410) highlighted that:

> … the internet and new media technologies have led to the emergence of cosmopolitan, reform-based movements in journalism, with the potential of creating a new public sphere avenue. The concepts of public journalism, civic journalism, citizen journalism and blogging … are tied to the central discourse that intends to diminish the gap between news and civic life and redefine the societal role of public sphere.

Gripsrud & Moe (2010) support the above fact when they posit that the mainstream media have always constituted the necessary infrastructure for the modern public sphere i.e. from the early print media to electronic media such as televisions and radio and now it has extended to the internet.

The fact that the cyberspace has become the ‘new’ public sphere, where citizens can converge and discuss matters of concern, the major concern will then be the impact of regulation on the internet where the latter seeks to expand or shrink the public sphere.

Democratisation of the public sphere and emergence of online public sphere has led to the rise of freedom of speech due to the use of pseudo names. Legal systems sometimes recognise certain on the freedom of speech, although it is a fundamental human right that is recognised worldwide. This is due to the fact that the freedom sometimes tends to conflict with other rights and freedoms such as libel, slander, pornography, obscenity, fighting words and intellectual property (Doomen, 2014).

Although there have been many contestations towards regulating the internet, governments in many countries has tried by all means possible to make sure that users of the internet are well protected from and making sure that the users themselves will not subject each other to harassment. The study strives to assess whether the Zimbabwean government seeks to safeguard their citizens from such malpractices through enacting the Cybercrime and Cybersecurity Bill into an act.

2.3 Conclusion

This chapter gave a detailed account of the literature review and theoretical framework on which this study is based upon.

CHAPTER THREE: RESEARCH METHODS AND METHODOLOGY

3.1 Introduction

This chapter discusses in detail the methodology and methods used to conduct this study.

3.2 Research Approach

The research utilised the qualitative research paradigm as qualitative research is a type of research that focuses on developing and understanding human systems, whether small or large (Yin, 2011; Savenye & Robinson, 2003). Mack et al (2005) further argues that qualitative research seeks to understand a given research problem or topic from the perspectives of the local population it involves. Qualitative approach abetted the researcher to make an unbiased analysis of how Zimbabwe is prepared to implement cyber laws in the country paying attention to the Cybercrime and Cybersecurity Bill of 2017.

Qualitative research method can easily be assessed for its quality and severity and they involve thorough descriptions of people's opinions and behaviour. It then can be argued that, human beings create their own reality and they can understand what they do depending on what they believe in. In this regard, one can argue that through the cyberspace, citizens create their own form of reality and interpret texts in the best way that gratifies their needs and beliefs. Media regulation and in this case internet governance most often work in favour of the few powerful in society hence this prompted the researcher to use qualitative research paradigm, as the Cybercrime and Cybersecurity Bill is a legislation that seeks to peek much into how people use the internet.

Qualitative method also seeks to answer questions about what, how or why of a phenomenon rather than concentrating on how many or how much is answered by quantitative research approach (Nuemann, 2002). In the same vein, the researcher had to use the qualitative research approach to answer the question of whether it is relevant for Zimbabwe to enact internet legislation and further answering the question of the feasibility of such a legislation in the country in the context of upholding human rights mainly freedom of expression. Qualitative research also helped the researcher to answer his proposed research questions as well as fulfilling the research objectives.

In addition, qualitative research approach focuses on naturally occurring events in natural settings, so that there is a view of what real life is (Berg, 1989). The government as the crafter and implementer of policies package it in a way that seem to make relevant and useful to the public. The approach was thus useful in conducting the study as it aided to examine if the bill helps to curb cybercrimes at the same time upholding user protection of privacy as well as freedom expression.

3.3 Population

The term population in a research refers to the total number of units from which data is collected (Parahoo, 2006). Burns & Groove (2003) further argues that these are all the units that satisfy the benchmark to be included in the study. Population in this research consists of various news articles from both the public and private media in relation to the bill as well as internet users i.e. the general public, law enforcing agents and members from the judiciary.

3.4 Sampling techniques and procedures

In coming up with a sample, the researcher used non-probability sampling specifically purposive sampling. According to Polit & Beck (2004) and Kothari (2004) a sample refers to a segment of the population, hence a sample is taken from the target population following specific criteria with the objective of creating representativeness with the target population. The researcher interviewed thirty people from Gweru to represent internet users, five police officers, two lawyers and three prosecutors. News articles from www.herald.co.zw, www.newsday.co.zw and www.dailynews.co.zw were used to represent the media industry. This was done to understand the contestations behind the bill under study as Latham (2007) clearly points out that the sample should be representative, in the sense that each sampled unit will represent the characteristics of a known number of units in the population.

The sample used in the research presented the full population, without reflecting bias towards specific attributes.

3.4.1 Purposive sampling

The study used purposive sampling. "Purposive sampling, also known as judgmental, selective or subjective sampling, reflects a group of sampling techniques that rely on the judgement of the researcher when it comes to selecting the units that are to be studied," (Sharma, 2017:751). The researcher used this sampling method to select a subset of various news articles that were published in the Zimbabwean media as well as selecting internet users as well as member of the police force and those in the judiciary. This is mainly because purposive sampling focuses on particular characteristics of a population that might be of interest to the researcher and these helps to answer the research questions (Marshall, 1996).

Purposive sampling involves the researcher handpicking respondents for the study (Lankshear, 2004). In this case, the researcher had to handpick police officers, lawyers, public prosecutors, citizens who had a bit of knowledge towards internet regulation as well news articles that commented directly on the bill under study. It can then be argued that purposive sampling involves units chosen based on distinct characteristics and terminate units that fail to meet the chosen criteria. It is against this background that the researcher used purposive sampling to single out units relevant to the study.

The researcher had to utilize purposive sampling as it provided the researcher with the justification to make generalisations from the sample that he studied (Sharma, 2017).

3.5 Methods of Data Collection

Data collection is the process of gathering and measuring information on varying interests in an established and efficient way that enables one to answer stated research questions, text, hypothesis and evaluate outcomes (Nastasi & Schensul, 2005). The main aim of data collection is to cover quality evidence that translates to rich data analysis and allows the building of convincing and credible answers to questions that have asked.

3.5.1 Interviews

The researcher used interviews to gather data for the study. He used telephone interviews and ushered out questionnaires to his respondents.

3.5.1.1 Questionnaires

It is against this background that this study implemented questionnaires as one of the key data collection instrument. This research focused on collecting data from the general populace from Gweru hence questionnaires were deemed appropriate, as there was a broad spectrum of respondents as well as its ability to provide for anonymity of the respondents hence the promotion of confidentiality.

A questionnaire is a research instrument consisting of a series of questions or other types of prompts for the purpose of gathering information from respondents (Gault, 1907). The researcher used questionnaires as a method of collecting data because responses were gathered in a standardised way so, questionnaires were more objective. Questionnaires were used to assess the public views in as far as the bill was concerned and their views on it being enacted into an act pertaining to issues of user protection of privacy as well freedom of expression.

3.5.1.2 Telephone interviews

A telephone interview is generally an interview conducted over the telephone. The researcher had to use telephone interviews in interviewing some of the public prosecutors and lawyers who were far away from the researcher.

Telephone interviews were used as cost cutting measure as well as saving time for the study. Members of the judiciary were very important in the study to give their opinions pertaining the bill. They were also interviewed on the importance of such as law in the country and also whether Zimbabwe will be able to implement such a law in this technological era.

3.5.2 Archival Collection/ Research

Archival research was used to gather information for this research because the relevant published articles on the bill are obtained from various media houses' websites as in this technological era archives are now found online. In this case, the researcher had to visit www.herald.co.zw, www.newsday.co.zw and www.dailynews.co.zw to pick relevant news stories regarding media practitioners to understand their reaction and opinion towards the bill. Archival collection is an integrated and conceptually informed procedure of locating, evaluating and systematic interpretation as well as analysis of sources found in archives (Fairclough, 1995).

The researcher used archival research because the data pertaining the media practitioners' reaction towards the bill was readily available hence understanding the standpoint of them in as far as the bill was concerned. This made the collection of data less time consuming and less costly and the problem of reactivity was minimised (Jackson, 2012). This was very vital in the research as it reduced bias because the data had already been collected hence researcher had no interaction with participants.

3.6 Methods of data analysis

3.6.1 Critical Discourse Analysis

Critical discourse analysis (CDA) was used as a method of analysing data for this study. Critical discourse analysis focuses on how the bias of social power, inequality and dominance are reproduced and revealed through verbal or non-verbal texts in the political or social context (Van Dijk, 1998). The use of CDA helped the researcher to understand whether Zimbabwe is really in need of the Cybercrime and Cybersecurity bill.

Bryman (2012) argues that CDA focuses on the role of language as a power resource for the expression of ideology and socio-cultural change. In this case, CDA enabled the researcher to understand and explain the reasons behind the creation and drafting of the bill under study.

Van Djik (1998) highlighted that CDA focuses on the way social power abuse, dominance and inequality are enacted, reproduced and resisted by text and talk in social and political context. CDA is also recognised by the Frankfurt scholars who questioned the social order and how capitalism is aimed at maintaining that social order hence the researcher had to use CDA to clearly spell out the unequal relations that take precedence in society, especially when the masses are ruled by those with the political muscles.

CDA is therefore employed in the study as it seeks to understand the discourse employed by the government to constantly pass their ideologies to the masses through legislations that seeks to subdue the general citizens. The texts that was subjected to CDA were the news articles that was obtained from media houses, which commented specifically of the bill as well text from the interviewees and the bill itself.

3.7 Methods of data presentation

The researcher used thematic data presentation. Data was presented thematically and was discussed in relation to the theoretical framework and literature review. This method allowed the researcher to interpret and clarify the research findings. The researcher used thematic data presentation as it goes beyond simply counting phrases or words in a text and moves on to identifying implicit and explicit ideas within the data.

3.8 Ethical considerations

Ethical issues are embedded in doing what is right or what is wrong. It is one of the major considerations of this research to conduct it in the right way. Crosswell (2003) asserts that when conducting a study, the researcher has the mandate to observe the desires, needs, rights and values of participants. It therefore means that respondents have the ultimate right to make reasonable decisions in as far as responses are concerned (Graziano and Raulin, 2004) as well as ensuring that the respondents identify the findings of the study as their experiences (Streubert and Carpenter, 2011). This was ensured by adhering to the principles which include; participants participated voluntarily and were not coerced, prospective participants were fully informed about the research and gave their consent, confidentiality and anonymity was guaranteed, respect was given to intellectual property and participants responded to the same key questions.

3.9 Conclusion

The chapter clearly outlined the research approach that was employed in conducting the study. Data gathering and sampling techniques and data analysis methods used in the study was also discussed.

CHAPTER FOUR: POLITICAL ECONOMY OF THE MINISTRY OF ICTs and CYBERSECURITY

4.0 Introduction

This chapter uses the political economy approach to discuss the drafting and production of the Cybercrime and Cybersecurity bill which is not yet a substantive law as it is not yet an act signed by the President, by the parent ministry, which is the Ministry of ICTs and Cybersecurity in 2017.

4.1 Historical Background of the Ministry of ICTs and Cybersecurity

The former Minister of Media and Publicity, Webster Shamu, was the first person to bring about the issue of regulating the internet sometime in 2012. In 2013, the Ministry of ICTs, Postal and Courier Services, which was later changed to Ministry of ICTs and Cybersecurity, started to draft the Cybercrime and Cybersecurity Bill to try to deal with issues related to cybercrime and cybersecurity. The then Parliamentary Portfolio Committee on ICTs Chairperson, Nelson Chamisa, was later in 2014 quoted by the *Daily News* arguing that the government had to move with speed to cover and protect the Zimbabwean populace from cyber bullying and other related cybercrimes (ZDI & MC, 2018).

The Ministry of ICTs and Cybersecurity currently headed by Supa Mandiwanzira was formed with the aim of developing an enabling environment for the creation of knowledge-based society that cut across all levels. The formation of the ministry was also fuelled by the need to monitor and regulate the cyberspace in the country, as cybercrimes were slowly gathering momentum. Zimbabwe first introduced a cybersecurity ministry in October 2017 called the Ministry of Cybersecurity, Threat, Mitigation and Detection which was later on merged with the Ministry of ICTs, Postal and Courier Services.

4.2 Vision Statement of the Ministry of ICTs and Cybersecurity

A vision statement as defined Grusenmeyer (2009) is an inspirational goal and statement of what an organisation strives to achieve hence it can be described as the picture of the future an organisation strives to reach. The Ministry of ICTs and Cybersecurity's vision is, "A knowledge based society with ubiquitous connectivity by 2020". In fulfilling this vision the ministry introduced the ICT Lab per school, which was aimed at introducing ICT from grassroots level, community information centres that were aimed at creating rural access centres and use the medium of ICT to promote community-based ICT applications. This was in line with the study as the internet is now used many people in the country despite their location and demography hence, there is need for them to understand policy in relation to their use of the internet, as most of them are ignorant of the media laws. The mission of the ministry helped the researcher to examine whether the government is doing enough in as far as regulating the internet at the same time protecting its citizens and giving them services they deem necessary.

4.3 Mission Statement of the Ministry of ICTs and Cybersecurity

A mission statement is a statement that highlights then fundamental purpose of the organisation by offering clarity on its operations and behaviour conduct (Grusenmeyer, 2011). The mission statement of the Ministry of ICT's and Cybersecurity is, "Exploiting the potential of Information, Communication Technologies and Cybersecurity (ICTCS) for sustainable socio-economic development in Zimbabwe". The ministry intends to achieve this mission through ICTCS governance, ICTCS infrastructure development, ICTCS research development, e-government, ICTCS access and utilisation and ICTCS corporate services. Socio-economic can be achieved when citizens are protected from harm by the government hence this mission statement helped the researcher to fully investigate the relevance of the Cybercrime and Cybersecurity bill.

4.4 Core Values of the Ministry of ICTs and Cybersecurity

Core values are a set of universal principles of an organisation's standards, behaviours and culture, which enable the right course of action (Anwar, 2013). The core values of the Ministry of ICTs and Cybersecurity are ethics, honesty, integrity, loyalty, passion, professionalism, transparency and trust.

4.5 Funding Mechanism

The government through the Ministry of ICTs and Cybersecurity funded the drafting of the Cybercrime and Cybersecurity bill. Stakeholders meeting were held in the country, putting together the views of various stakeholders and the general citizens. The Minister of ICTs and Cybersecurity, Supa Mandiwanzira was quoted by *Newsday* saying, "On the issue of Cybercrime and Cybersecurity bill, consultants were hired to do the drafting and paid not more than $10 000".

As the government funded the whole process of drafting the bill under study and gathering views gives the sitting government the power to determine the outcome as they would want the bill to be in line with its ideology as the saying 'he who pays the piper dictates the tune'. In terms of Section 141 of the Zimbabwean Constitution, Parliament is mandated to engage the public, its legislative and other process of its committees and ensure that interested parties are consulted about bills.

Bills should always be interrogated to make sure that they are not only constitutional but also address matters of national interest, hence they have to be scrutinised through debates. In line with this, through the Ministry of ICTs and Cybersecurity, the parliament of Zimbabwe engaged citizens and various stakeholders on the draft bill, taking note of all suggestions they raised. However, inadequate budget that is sometimes allocated to parliament hinder the process to go as planned as for instance the consultative meetings on the bill was supposed to be done nationwide but ended up being conducted in Harare, Bulawayo and Gweru only.

4.6 Ministry of ICTs and Cybersecurity's structure

The Minister, who is arguably the ministry's vision bearer, heads the structure of the Ministry of ICTs and Cybersecurity and the current Minister is Supa Mandiwanzira. He is collectively responsible for the conduct of the government as a whole. The Permanent Secretary, who is Engineer Sam Kundishora, follows the Minister. The permanent secretary acts as the policy advisor to the minister, as he provides objective advice on issues related to policy, on the government's options in dealing with them and on the implications of each option. The advice given to the minister requires a complete understanding of complex technical, managerial, legal and financial issues. He also partake in the collective management of the public service through serving on special task forces investigation policy questions or matter of government organisation as well as heading corporate projects and joint committees.

The Principal Director, who is Simon Chigwamba, follows the permanent secretary and five directors follow him. The Directors are Dr Chirume who is the head of ICT services, Mrs Chingonzo who heads the Policy Cordination, Development and E-Government Department, Mr Nyamhuri who heads the department of Research Infrastructure Development and Management, Mr Saburi who heads the Finance, Administration and Human Resources Department and Mrs Ngwangwa who is the Legal Advisor in the Ministry.

4.7 Departmental Structure of the Ministry of ICTs and Cybersecurity

The Ministry consists of six viable departments.

4.7.1 Cyber Security Department

The cyber security department has a plethora of functions. The functions of the department includes developing the legal framework and the laws to govern the practice of cybersecurity in the country, ensuring in collaboration with the Ministry of Justice and the Ministry of Home Affairs and their institutions, the successful arrest and presentation of offenders.

In addition, it has also the task of monitoring, in cooperation with other security services, cyber threats and respond to cybersecurity incidents that threaten the Zimbabwean national security, economic and social interests. Establishing and supervising the national institutions that will implement the cybersecurity policy and programs is also another function of the department. It is further responsible for coordinating cybersecurity policy activities with all other sectors of government, promoting the ethical use of ICT and cyberspace and fostering cooperation between the public and private sectors in the establishment and maintenance of national cyber security.

Lastly, it has the mandate to ensure international cooperation with other nations including inter-governmental organisations such as the United Nations. In this regard, to participate in the International Telecommunications Union’s Cyber Security agenda thereby making it possible to prosecute cross border cyber threats actors in Zimbabwe or in other countries from which they actualise their threats. This thereby helped the researcher to investigate the neediness of a cyber-law in Zimbabwe if the country has already put up such an institution to monitor and govern the use of ICT and the internet at large.

4.7.2 Policy Coordination, Development and E-Government Department

This department is responsible for creating and developing necessary policies, regulatory frameworks and strategies that augment endowment of ICT and cybersecurity. It also has the mandate to monitor the conduct and running of ICT and cybersecurity including the formation of principles and their implementations. Promotion of the interests of users of ICTs and the cyberspace in respect of prices, quality and variety of services provided and the monitoring of operations of state owned enterprises under the Ministry is another function of the department.

4.7.3 Infrastructure Development and Management Department

This is yet another department in the Ministry of ICTs and Cybersecurity that has the task of developing, managing and maintaining central government ICT infrastructure, developing supportive and enabling communications infrastructure to ensure equitable access tom ICTs by all citizens including disadvantaged and vulnerable groups and rural communities.

4.7.4 Administration, Finance and Human Resources Department

The department's key result areas are managing and safeguarding public finance, property and human resources and improve service delivery

4.7.5 Legal Department

This department's main role is to advise and represent the ministry on legal issues.

4.7.6 Research, Development, Monitoring and Evaluation Department

This the last department in the Ministry which is responsible for evaluating the impact of ICTs and cybersecurity on social and economic development and introducing and enforcing stringent quality service standards in the provision of ICTs and Cybersecurity.

4.8 Political Economy of the Ministry of ICTs and Cybersecurity

Media moguls use the mass media to endorse the interests those in high power positions (Curran & Guveritch, 2005). In this regard, it can therefore be argued that the Ministry of ICTs and Cybersecurity drafted the Cybercrime and Cybersecurity bill in a bid to preserve the ideology of the ruling party, ZANU PF, as the citizens through social media were challenging it. McChesney (2000) noted that political economy of communication mainly focuses at how ownership and ownership and government policies influence media behaviour of content, it also focuses of how media and communication system challenge and reinforce the existing ones. The inclusion of the government in coming up with bill clearly depicts that it is indeed an interested party as it wants to avoid Arab spring like kind of revolutions in Zimbabwe. When the sitting government plays a pivotal role in the formation of policies, the question that comes into one's mind is whose interest and whose values are encouraged in the policy formulation; hence, in this regard the Ministry's inclusion in the formulation of the bill becomes debatable as a ZANU PF minister heads the Ministry.

Media organisation and government branches work as tools to achieve political end games in Africa. Herman and Chomsky (1988) asserts that ownership can be influential in bringing upon the ideologies of those in the realm of power and bring ideologies into prominence. This reveals that through ownership patterns the government impose its ideas on the masses through instruments that are very popular with the people. The Cybercrime and Cybersecurity bill is can be argued to have been designed to impose new laws on the citizens of Zimbabwe. Therefore, every amendment and design of a law and ownership in control is for gain political mileage. Visibly, new technologies are taking over from old media as being the most influential and most used in today's communities and its popularity has been noticed through social media uprisings in Zimbabwe like the '#ShutZimdown' where online social media platforms were used to expose the government's shortcomings. Therefore, the new bill under study wants to make sure that ultimate power is achieved when it comes to the use of online social media platforms.

4.9 Conclusion

The chapter discussed the political economy of the Ministry of ICTs and Cybersecurity, its core values, mission and vision statements. It can be argued the Ministry's role in funding the creation of the bill under study has an impact in its outcome if the President signs it into an act.

CHAPTER FIVE: DATA PRESENTATION AND ANALYSIS

5.0 Introduction

This chapter presents and discusses the findings of the research and data was presented thematically. The bill is currently waiting for the President's signature for it to be a binding law or an act.

5.1 Cybercrime and Cybersecurity Bill vital for the protection of online users

From the data that was gathered, the researcher found out that the bill under study is indeed important in Zimbabwe as the cases of cybercrime like cyber-bulling are gaining momentum day by day. The researcher noted that before the Ministry of ICTs and Cybersecurity crafted the bill, there had been calls from various individuals, corporations and government departments to put in place a legislative framework for cybersecurity as the laws that are currently in place do not directly address issue of cybercrime and cybersecurity. The bill also came after the legal fraternity had raised issues that dealing with cases nowadays is becoming a mammoth task. They cited that evidence to presented in courts is now on cell phones and computers and it is inadmissible hence there was need for laws need to be enacted.

A huge call was also made in 2013 after the Baba Jukwa saga on Facebook where the perpetrator allegedly posted information that was against the sitting government and against the former President, Robert Mugabe (Mutetwa, 2015) and in the same year the drafting of the bill commenced.

5.1.1 Analysis of the Cybercrime and Cybercrime bill

The increasing rate of cyberbullying and dissemination of pornographic material on social media has become rampant in the country hence a binding law is really needed and is very relevant in the country to make sure the perpetrators of online crimes are brought to book and face the wrath of the law. Clauses in the bill highlights that the bill is intended to guard against national security, crimes against the state as well as organisations and individuals.

Section 19 (1) of the bill notes:

> Any person who unlawfully and intentionally by means of a computer or information system makes available, broadcasts or distributes a data message containing any intimate image of an identifiable person without the consent of the person concerned causing the humiliation or embarrassment of such person shall be guilty of an offence and liable to a fine not exceeding level ten (US$700) or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment.

Zimbabwe has of late seen the increase in the dissemination of ‘sex-tapes’ via online means and women were the main disadvantaged group hence this bill is meant to guard against such a group and making sure that everyone regardless of gender is rightfully protected by the law.

In addition, the bill also intends to protect the transmission of data messages inciting violence or damaging property, sending threatening data messages, cyberbullying and harassment and the transmission of false data messages intending to cause harm among a plethora of things but many questions arise. The main question will be whether the bill will be used to protect everyone or it will only protect those in power and disempower the masses who has of late grasped the use of the internet to air their views. This prompted MISA (2017) argue that bill is just focused on the criminalisation of cybercriminals but at the same time quiet on the need for protection of individual liberties, accountability in the process of combating cybercrime. In this regard there is need to consider an expansion on the purpose of the bill to include respecting of individual rights in the process of collection of evidence or prosecution of cybercrimes and mention of fair trial rights to everyone.

In cementing the above argument, ZDI & MC (2018) highlighted that although the bill is very important in the country there is need for the revision of the bill before it is enacted into law. They argued that political context of the bill dictates that in crafting the bill, the government was driven more by its fear of then citizen and civic pressures unveiled by unsuppressed internet freedom than amplifying citizen’s security when exercising their freedoms online. This then means that the government drafted the bill in trying to marginalise internet users.

They noted:

> Although with some progressive attempts curb cybercrimes, the Cybercrime and Cybersecurity bill was to a greater extent, crafted with an authoritarian intentions to: (i) instigate self-censorship among citizens and thereby cushioning government against citizens oversight (ii) increase government authority and ability to 'legally' violate privacy thereby enabling state interference with communications online and (iii) contain, dissuade an clampdown potential social media revolutions and demonstrations that had proven to be presenting a real platform for citizen's will to be done (ZDI &MC, 2018: i).

Currently, section 162 to 168 of Chapter 8 of the Criminal Code (Codification and Reform) Act tries to deal with the issues of unauthorised access and use of computers, passwords and manipulation. This piece of legislation lacks the real know how on how to deal with perpetrators of cybercrime as it does not speak directly to them hence making it hard for the police and courts to persecute such offenders. Another act in the land, which has tried to address issues related to cybercrime is the Postal and Telecommunications Act (Chapter12:05) which makes it an offence for one to disseminate through a telephone any threatening message or a message which is offensive, annoying or false, indecent, obscene or of threatening character. The word 'telephone' used in the act is making it easier for cybercrime perpetrators to go scot free in this technological era where people no longer commit these crimes on their telephones.

Many citizens and organisations in Zimbabwe have become victims of cybercrime on social media. Notable examples include Lydia Zvaipa who is the mother to the late Movement for Democratic Change (MDC – T) leader Morgan Tsvangirai who fell victim after a video of her ranting that she did not want to see her widowed daughter in law and Nelson Chamisa at the funeral of her son and that she would commit suicide if the duo were to attend. Also sometime January 2017, OK Zimbabwe suffered a $70 000 hit in their finances after a man from Chitungwiza hacked in company's Money Wave System. Many politicians and government ministers in the country has also fallen victims of cybercrime hence the introduction of the bill has been one of the things which is long overdue in the country. Mutsvairo (2016) concurs with this argument as he highlighted that the internet is now being used as tool for hate speech, intolerance and has over the years increased the disempowerment of those citizens who lack access or the ability to use the internet to its full effect. This then shows that indeed the bill is very vital in trying to make sure that everyone's rights are protected thereby promoting equality among citizens and the powerful in society.

5.1.2 Newspaper analysis of the Cybercrime and Cybersecurity bill

Most Zimbabwean citizens own or have access to a gadget that is compatible with internet making it easier for cybercrimes to be committed using these gadgets. In an article published by the *Newsday* on March 1, 2018 by Kennedy Nyavaya titled 'Cyberbullies prowl due to lax law enforcement' it was discovered that indeed the current legislation in Zimbabwe is relaxed in terms of dealing with cybercrimes. Part of the article reads:

> From one smartphone and computer, like a wildfire it did not take long before Gogo Tsvangirai started trending on different online platforms, becoming an instant victim of the rampant growing cyberbullying trend in the country. The ardent use of communication devices, especially smartphones and subsequent rise of social media users had resulted in the creation of unrestrained communication channels between people from different places and backgrounds. The absence of stern laws to regulate the sending of messages back and forth has resulted in abuse by some users who cause untold suffering to others by relaying fake news, insults or degrading messages.

The article further reveals that, in Zimbabwe the delay in passing the Cybercrime and Cybersecurity bill into law prompts the idea that there is not much political will to curtail the growing phenomenon of cybercrimes. However, the Minister of ICTs and Cybersecurity, Supa Mandiwanzira was also quoted saying, "It (the bill) is in the Attorney General's office where they are also looking at other draft bills with the wisdom of combining them into a substantive law".

In another article in *The Herald* of 09 June 2017 titled 'Cyber law not linked 2018 polls: Minister', the now Minister of ICTs and Cybersecurity Supa Mandiwanzira was quoted saying, "It is important that we have this law as of yesterday, not tomorrow and not today because our people are being abused. They are vulnerable and we need to protect them". He also emphasised that when enacted into law, the bill will assist the judiciary when dealing with crimes committed on social media. This shows that there are certain people in society who cannot stand up for themselves and have succumbed to social media abuse but could not protect or defend themselves due to vulnerability hence a law will be necessary to make sure that the disempowered will be protected by law.

5.1.3 Views of law enforcing agents on the bill

The law enforcing agents, who were also interviewed, concurs that for sure the bill is one long overdue as it was hard for them to deal with such issues due to the lack of proper legislations. One police officer noted, “This bill is very important as many people are abused online almost on a daily basis due to the increase in internet services and the advent of social networks.” This shows that although the internet seems to offer equality, there users who are superior than others hence making the inferior ones subjected to all forms of abuse hence a binding law will be necessary to make sure the marginalised are well protected.

One lawyer who was interviewed noted that:

> Such a law is necessary considering that people are abusing their freedom of expression on social media platforms and tarnish other people’s integrity and reputation. The introduction of the bill is very relevant in curtailing social media abuses. The current legislation is not fully curbing cybercrimes. I think it is because social media platforms and their abuses existed way after these statutes were established hence it is therefore necessary to enact new laws to meet the prevailing situation and in this case the Cybercrime and Cybersecurity bill.

One can therefore argue that for sure the bill under study is very relevant in Zimbabwe as it seeks to protect citizens from those who tend to use the internet for promiscuous purposes hence making all internet users equal regardless of social status, gender, age, race, ethnicity etc. if it is passed into an act.

Also from the findings, the researcher managed to find out that the some people in the judiciary are also calling for the enactment of the bill into law. One public prosecutor, Clement Kuwanda who was interviewed noted:

> The current legislation is lagging behind in terms of bringing to book perpetrators of cybercrime hence this bill will help in making sure that justice

> will prevail. Cybercrime is on the rise in Zimbabwe and individuals who use pseudo names such as Baba Jukwa stir violence in Zimbabwe, which is indeed a crime. The bill will help protect Zimbabwe, maintain peace, order and stability.

5.1.4 Internet users' perceptions on the bill

In addition, some internet user who answered questionnaires also echoed the same sentiments that indeed the bill was crafted at the right time. Respondents highlighted that the internet is slowly becoming a menace in society labelling it a 'hub of promiscuity' where some individuals are more dominant than others are, also making people to abuse their internet freedom and infringe other users' freedoms . One respondent said, "Internet usage is increasing day by day hence there is need for proper regulation for the purpose of order and also to avoid abuse by users".

However, another responded totally refuted the idea of regulating the internet through the enactment of the bill as she cited the government would only want to exercise its power and silence opposition parties who has of late taken the social media by storm. She noted:

> Cybercrimes are rampant in the first world countries where almost everyone has access to the internet. Yes, there may be a little trolling but I do not think it is worth such a bill. I feel like they just want to silence political critics. The government just wants to invade alternative sphere. Without mentioning the Baba Jukwa issue, I have not heard any trial on cybercrime so it is either there is no cybercrime or the current legislation is doing absolutely nothing.

The findings proved that for real Zimbabweans are in need of such a law due to the ever-changing types of cybercrimes as Madondo (2017) argued that indeed the country is ill prepared for cybersecurity and is very much vulnerable to cyber terrorism. However, there are several calls that the bill should be revisited first to ensure that there is equality among all individuals and stakeholders before enacted into law. Data gathered also showed that the government should exercise its power in making sure that the bill should be enacted into law very soon as it has taken ages for the bill to be signed into an act due to the change of Ministers. However, some respondents believed that the ZANU PF government is trying to impose its ideology on citizens and exercise its powers to manipulate and silence the audience who utters bad comments about it.

5.2 Cybercrime and Cybersecurity bill, a threat to freedom of expression

5.2.1 Law enforcing agents' view

The constitution of Zimbabwe under section 61 (1) guarantees freedom of expression and freedom of the media which includes freedom to seek, receive and communicate ideas and other information and the freedom of artistic expression and scientific research and creativity. The researcher found out that although the country needs such a law, the law should protect this constitutional right as people feel it tends to infringe this right. This is supported by ZDI & MC (2018) when they argued that the Cybercrime and Cybersecurity bill is quiet on safeguarding citizens' liberties and enhancing accountability in the process of trying to curb cybercrimes. Social media in the country has managed to break all odds that might have hindered people to discuss issues of governance freely hence, most people believed that might have been crafted to curtail them from discussing such issues.

A lawyer who was interviewed highlighted that the bill has to make sure that it does not infringe people's right to freedom of expression. He noted:

> I personally think that the bill will have a negative impact on freedom of expression. Our country is one of the countries with barbaric media laws which constraints media practice. Government has a tendency of abusing the media in the name of national interest, security and safety. This then means that if the bill is enacted into law will be used to silence the citizens and the media by violating freedom of expression.

A member of the police force who was also interviewed also supported the above argument as he said:

> The majority of Zimbabwe has taken the internet as their point of expression on sites like Facebook and WhatsApp hence if enacted into law into the law the bill will hinder freedom of expression and will stop citizens from criticising the government online because they cannot do it in the mainstream media due to stringent media laws.

Therefore, one would then argue that the government might use its powers to subjugate freedom of expression and strips off the public and the media the power to create and disseminate information on the internet. The internet has of late empowered citizens to air their concerns to the government and has broken the gap between the powerful and the subaltern and it is believed that through such a law the government is trying silence social media activists thereby disempowering them.

5.2.2 Internet users' perceptions

Furthermore, from the data gathered from internet users, the researcher noted that citizens fear for their freedom of expression as they highlighted that it is the government's agenda to make them silent on the social media. The government of Zimbabwe has of late reacted and passed laws depending on the prevailing situation, this has seen the enactment of law Public Order and Security Act, Access to Information and Protection of Privacy Act among others, whenever it felt threatened (Mukasa, 2003). Most respondents felt that if enacted into law the bill would favour only the top echelon at the same time marginalising the masses. However, some respondents believed that bill had a huge impact on freedom of expression in the era of the former President, Robert Mugabe as they highlighted that the current President, Emmerson Mnangagwa's reign has seen a shift in as far as freedom of expression is concerned. One respondent said:

> The bill will somehow affect our freedom of expression because you may have freedom of speech but there is no guarantee of freedom after speech. The bill is an ideological repressive tool that seeks to shape how we will use the media hence there is need for the government that this bill tally well with the current constitution.

Another respondent noted:

> The internet had provided a good public sphere, so with the coming in of such a legislation will limit on what we can say hence people will end up being prosecuted for expressing our views. In addition, we are going to have problems with the legislation as it will protect the interests of government and the general citizens are stripped off all their powers to freely create and

disseminate news hence we need to be aware on whose interest the bill is going to protect.

5.2.3 Newspapers' view

In an article by the *Dailynews* on 10 October 2016 titled 'Artists and Cybercrime bill' highlighted that, "If this this law is to protect the society it is fine but if it is to incriminate and persecute, it will face ideological and technological resistance of unpredictable forms". It was also noted in the article that bill goes against the spirit of expanded media freedom and the protection of online users in an open, democratic and transparent society as envisaged by the constitution. Feltoe (2003) concurs with this argument as he argued that freedom of expression is recognised worldwide as a major value of the community. Freedom of expression is vital in a democratic society as it allows the free flow of ideas and information in a society hence the government should not by whatsoever means try to deny the citizens this constitutionally guaranteed right. The idea of making the draft accessible and encoded by the public before enacted into an act is a clear indication that the government want citizens to fear that they are being monitored and desist from criticising the government on social media.

5.3 Implementation of the legislation will be a mammoth task

From the data gathered, the researcher noted that although Zimbabwe is in dire need of cyber laws and calling for the enactment of the Cybercrime and Cybersecurity bill into an act, the implementation of the legislation will be a very huge task. Dealing with cybercrimes needs a lot of time, money, technology and expertise hence it might be hard for Zimbabwe to implement such a law. As highlighted in Chapter 2, that the internet is gaining popularity almost everyday and its services and offers are growing very fast, due to its cheap hardware and wireless access. This then means that the growing number of individuals connected to the internet has also led to the increase in the number of targets and offenders hence it is very difficult to be able to estimate the number of people who uses the cyberspace for illegal activities. The researcher also managed to realise that although internet usage rates are a bit low in developing countries, Zimbabwe included, promoting cybersecurity is not easy as offenders can commit offences from around the globe hence the increasing number of internet users causes difficulties for the law enforcing agencies because it is relatively difficult to automate investigation processes.

A lawyer who was interviewed said:

> Zimbabwe is currently having trouble in catching up with the digital media hence it will be very complicated and costly to the nation to track down criminals and bring them to book. The nation does not have adequate resources to implement new laws. As it stands, the police are unable to track the origins of cyber criminals. It can be noted that cybercrime villains are more advanced in terms of knowledge, technology and escaping scot-free.

From the data gathered, the researcher also noted that international dimensions would be another tool that will hinder the smooth implementation of the bill, if it is passed into an act. Many data transfer processes affect more than one country; hence, if offenders and victims are geographically located in different countries, the investigations will then need the cooperation of law enforcing agents in all countries affected as national sovereignty does not allow investigations within the territory of different nations without the permission of local authorities. This then means that cybercrime investigations needs the assistance and involvement of authorities in the nations involved. In addition, the usage of pseudo names and privacy policies was also cited as major challenges of investigating and implementation of the bill in Zimbabwe. One public prosecutor noted, "The use of pseudo names by internet users will make it very hard for us to deal with cybercrimes as there will be need for verification of user identity and getting such information is not that easy".

This argument was cemented by another public prosecutor who highlighted that:

> I do not think that Zimbabwe will be able to implement such a legislation as the government does not have access to control to some of the social media platforms like Facebook, Twitter and WhatsApp as the messages will be encrypted, therefore they will face challenges in tracing the offenders.

This then means that although the government might want to protect its citizens from cybercrimes through enacting the bill under study into an act but it will face many challenges in bringing the criminals to book hence it will end up being used to tackle silly issues and leaving bigger problems unattended. This also might end up in the disempowering of the masses, as they will have nowhere to discuss their concerns after learning about the offences in the bill.

5.4 Conclusion

This chapter manage to analyse the data that was conducted from the research population and analysed it through Critical Discourse Analysis. The researcher managed to note that Zimbabweans are really in need of the Cybercrime and Cybersecurity bill in trying to make sure that all people are equal on the cyberspace as well as in airing their disgruntlements. However, a call was made to the government to make sure that the bill suit the needs of all affected parties before it is enacted into a binding law.

CHAPTER SIX: CONCLUSION AND RECOMMENDATIONS

The study investigated the relevance of the Cybercrime and Cybersecurity bill, 2017. The research further examined the extent to which Zimbabwe can be able to implement the bill, if enacted into an act without infringing citizens' right to privacy as well as freedom of expression as enshrined in the country's constitution. The researcher discovered that such a legislation is needed but there has to be amendments first to suit everyone in the country.

Qualitative research paradigm was used in carrying out the study. The researcher used this research paradigm as it helped him to understand his research problem from the perspective of the population that was involved. It also helped the researcher to make an unbiased analysis of whether Zimbabwe is in need of the bill or not. However, the approach was time consuming especially when collecting and analysing data from the samples of the population that the researcher had chosen.

The researcher used telephone interviews, issued questionnaires and did archival research in search of different views pertaining to the relevance of the bill in Zimbabwe. There was consensus amongst all respondents that indeed the bill was very important in trying to curb cybercrimes in the country, which is currently getting rife day by day. However, some respondents and reviewed articles highlighted that there is need for the government to first revise the contents of the bill before it is enacted into a fully fledged law as they fear that the general masses will be disempowered in their use of social media to its full thereby being denied their right to privacy and freedom of expression. It was also noted that the government of Zimbabwe is reactive rather than proactive as the bill was drafted just after the Baba Jukwa saga towards the 2013 harmonised elections (Mutetwa, 2016).

Literature from various scholars was used in coming up with themes that were relevant to the study. Mhiripiri and Chari (2017) denoted that the society needs to be well equipped with literature in relation to law and ethics in the new media. They further articulate that social media has ushered in new journalistic practices which has made old laws useless and has rendered media regulatory authorities as sitting ducks hence there was need for an intervention in making sure that the creation and dissemination of content is done in the right way. Chibuwe (2012) highlighted that political and commercial interest take the centre stage in the crafting of media policies. Mutsvairo (2016) further highlighted that digital technologies have disrupted the manner in which media content is consumed worldwide and has led to the disempowerment of those citizens who lack access or the ability to use these social media platforms to full effect. Packard (2010) also noted that media regulation has also shifted to the digital media and people should stop thinking of media regulation as a thing of the traditional media.

The researcher used the democratic participant theory, democratisation of the public sphere and technological determinism in the technological era as theories in theorising the conceptual framework.

Data was presented through thematic data presentation method and was analysed using the Critical Discourse Analysis, as the researcher was worried with issues to do with how the bill seeks to maintain power and equality, marginalisation and disempowerment of the individuals in the society as shown through the bill’s encoding. Data themes were derived from responses and criticism that were given by the law enforcing agents, members of the judiciary, news, internet user as well as news articles that commented on issues to do with the bill.

The theories, methods and methodology used in the study helped the researcher to understand whether the bill is relevant or not in Zimbabwe. The theories also helped the researcher to lay a foundation of the study. The methods and methodologies helped to make sure that useful data is gathered timeously and at a lower cost.

Recommendations to further studies

The researcher also recommends to the future researchers to examine how the bill will try to protect the journalist profession as this profession is now under threat due to the citizen journalism and bloggers who sometimes breach some ethical codes and laws without being brought to book.

The research investigated the relevance of the introduction of the Cybercrime and Cybersecurity of 2017 in Zimbabwe and the researcher found out that the indeed there is a need for the bill to be urgently upgraded into an act as cyber offences are taking precedence.

The first chapter constitutes the introduction to the study whilst the second chapter encompasses literature review and theoretical framework. Research methods and methodology were presented in the third chapter, whilst chapter four gave a political analysis of the Ministry of ICTs and Cybersecurity. Research finding were thematically presented in Chapter 5 and the last chapter gave concluding remarks as well as recommendations to future studies.

REFERENCES

Adolf, M., & Wallner, C. (2005) "Probing the public sphere in Europe. Theoretical problems: Problems of theory and prospects for further communication research". Paper presented at the first European Communication Conference 24. Amsterdam, Netherlands

Akuta, E., Ong'oa, I., & Jones, C. (2011) "Combating Cyber Crime in Sub-Saharian Africa: A Discourse on Law, Policy and Practice". *Journal of Peace, Gender and Development Studies*, 1 (4), 129-137

Anwar, J. (2013) "Ideology, Purpose, Core Values and Leadership: How they influence the Vision of an Organization? *International Journal of Learning & Development*, 3 (3), 168-184

Aveyard, H. (2010) *Doing a literature review in health and social care: A practical guide* (2nd ed.). Berkshire: Open University Press

Belk, R., & Noyes, M. (2012) *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Polic*y, US Department of Defense: Havard Kennedy School

Berg, L. B. (1989) *Qualitative Research Methods for the Social Sciences* (7th ed.), California: Long Beach

Bruns, A. (2008) *Gate watching, Gate-crashing: Futures for Tactical News Media.* In M. Boler (Ed.), Digital Media and Democracy: Tactics in Hard Times (pp. 247-270), Cambridge: MIT Press

Bryman, A. (2012) *Social Research Methods* (4 ed.), Oxford: Oxford University Press

Burns, S. N., & Grove, S. K. (2003) *Understanding Nursing Research* (3rd ed.), Philadelphia: Saunders

Chandler, D. (2000) *Technological or Media Determinism*, United Kingdom: Aberystwyth University Press

Chari, T. (2013) *Rethinking the democratization role of online media: the Zimbabwean Experience*, In Olorunnisola, A. & Douai, A. (eds.), New Media influence on social and political change in Africa, USA: IGI Global

Chatora, A. (2012) *Encouraging Political Participation in Africa: The Potential of Social Media Platforms*, Institute for Security Studies: ISSA Africa

Chibuwe, A. (2012) "The digital public sphere: challenges for media policy", *Critical Arts: South-North Cultural and Media Studies*, 26 (4), 621-627

Chitauro, G. (2015) *Cyber Laws Vital for Zimbabwe*, retrieved November 28, 2017 from TechnoMag: http://www.technomag.co.zw

CIPESA, (2016) *State of Internet Freedom in Zimbabwe: Charting Patterns in the Strategies African Governments Use to Stifle Citizens' Digital Rights*, Africa: CIPESA

Crosswel, J. W. (2003) *Qualitative, Quantitative and Mixed Methods Approaches*, California: SAGE

Curran, J., and Gurevitch, M. (eds) (2005) *Mass Media and Society*, London: Hodder

Doomen, J. (2014) *Freedom and Equality in liberal Democratic state*, USA: Bruyant

Fairclough, N. L. (1995) *Critical Discourse Analysis: The Critical study of Language*, Harlow, UK: Longman

Feltoe, G. (2003) *A guide to media law in Zimbabwe*, Harare: Legal Resource Foundation

Graziano, A. M., & Raulin, M. I. (2004) *Research Methods: A Process of Inquiry* (5 ed.), Boston: Pearson

Gripsrud, J., & Moe, H. (2010) *The digital public sphere: Challenges for Media Policy*, Sweden: Nordicom

Grusenmeyer, D. (2009) *Mission, Vision, Values & Goals:* unpublished

Habermas, J. (1989) *The structural transformation of the public sphere: an inquiry into a category of bourgeois society,* Cambridge: MIT Press

Halder, D., & Jaishankar K. (2011) *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations,* Hershey: IGI Global.

Hansen, L., & Nissenbaum, H. (2009) "Digital Disaster, Cyber Security and the Copen Hagen School". *International Studies Quarterly*, 53 (2), 1155-1175

Hartley, J. (2008) *Journalism as a Human Right: The Cultural Approach to Journalism*. In M. Löffelholz and D. Weaver (Eds.), Global Journalism Research: Theories, Methods, Findings, Future (pp. 39-51), New York: Peter Lang

Hartley, J. (2009) *Journalism and Popular Culture*. In K. Wahl-Jorgenson and T. Hanitzsch (Eds.), Handbook of Journalism Studies (pp. 310-324), New York: Routledge

Hauser, G. (1998) "Vernacular dialogue and the rhetoricality of public opinion". *Communication Monographs*, 65 (2), 83 – 107

Herman, E. S., and Chomky, N. (1988) *Manufacturing Consent: The Political Economy of the Mass Media*, USA: Pantheon Books

Herselman, M., & Warren, M. (2004) "Cyber Crime Influencing Businesses in South Africa". *Journal of Issues in Informing Sciences and Information Technology*, 1 (3), 253-266

Jackson, S. L (2012) *Research Methods and Statistics: A Critical Thinking Approach,* California: Wadsworth Publishers

Javuru, K. (2013) *New Media and the changing public sphere in Uganda: Towards deliberative Democracy?* In Olorunnisola, A. & Douai, A. (eds.), New Media influence on social and political change in Africa, USA: IGI Global

Kang, C. (2010, December 7) *FCC net neutrality plans gets picked apart from all sides*. The Washington Post: Washington DC

Kapor, M. (1993) "*Where is the digital highway really heading?"* Wired July/August: 94

Karppinen, K. (2013) “Uses of democratic theory in media and communication studies”. *Observatario (OBS) Journal*, 7 (1), 001 – 017

Kasoma, T. (2013) *Press Freedom, Media Regulation and Journalists’ Perceptions of their roles in Society: A case of Zambia and Ghana.* In Olorunnisola, A. & Douai, A. (eds.), New Media influence on social and political change in Africa, USA: IGI Global

Keane, J. (2004) *Structural transformation of the sphere*, In Webster, F. (ed.), The Information Society Reader, New York: Routledge

Kothari, C. R. (2004) *Research Methodology, Methods and Techniques*, New Delhi: New International (P) Limited Publishers

Lankshear, C. (2004) *A Handbook for Teacher Research: From Design to Implementation. Maidenhead*, UK: Open University Press

Latham, G. P. (2007) *Foundations for organised science. Work Motivation: History, theory, research and practice*, Thousand Oaks: Sage Publications

LeCompte, M. D., & Preissle, J. (1993) *Ethnography and Qualitative Design in Educational Research (2nd ed.)*, New York: Academic Press

Livingstone, S. (2003) *The changing nature of audiences: from the mass audience to the interactive media user*, Oxford: Blackwell

Maat, S. (2009) *Cybercrime: a comparative law analysis*, unpublished LLM thesis: University of South Africa

Mack, N. Woodsong, C. MacQueen, K. M. Guest, G. Namey, E. (2005*) Qualitative Research Methods: A Data Collector’s Field Guide*, North Carolina: Family Health International

Madondo, T. (2017) *Exploring cyber security threats in Zimbabwe*. POLICY BRIEF N0. 8 – November 2017

Majome, M. T (2017) *Everyday aspects of cybercrime*, retrieved October 28, 2017 from Newsday Zimbabwe: http://www.newsdayzimbabwe.co.zw

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatiuschtschenko, E. (2013) *Comprehensive Study on Cyber Crime*, New York: United Nations Office on Drugs and Crime

Marshall, M. N. (1996) *Sampling for Qualitative Research, Family Practice*. 13 (1), 522-525

McChesney, R. W. (2000) *The political economy of communication and the future of the field of Media, Culture & Society,* 22(1), 109-116

McNair, B. (2006) *Cultural Chaos: Journalism, News and Power in a Globalised World,* London: Routledge

McQuail, D. (1983) *Mass Communication Theory*, SAGE: London

Mhiripiri, N. A., & Mutsvairo, B. (2013) *Social media, New ICTs and the challenges facing the Zimbabwean democratic process,* In Olorunnisola, A. & Douai, A. (eds.), New Media influence on social and political change in Africa, USA: IGI Global

Mhiripiri, N.A., & Chari, T. (2017) (eds.) *Media law, ethics and policy in the digital age,* USA: IGI Global

MISA-Zimbabwe & Digital Society Zimbabwe. (2016) *Computer crime and Cybercrime bill: A Framework for Zimbabwe*. Retrieved March 20, 2018, from http://crm.misa.org/upload/web/Computer%20Crimes%20&%20Cyber%20Crimes_Framework_Zimbabwe.pdf

MISA-Zimbabwe. (2015) *Internet Governance Multistakeholder Conference Report 2015: Supporting Free and Secure Online Expression and Access to Information in Zimbabwe*. Harare: MISA-Zimbabwe

MISA-Zimbabwe. (2016) *Computer crime and cybercrime bill: A framework for Zimbabwe*, Harare: MISA Zimbabwe

Mukasa, S. D. (2003) "Press and Politics in Zimbabwe". *African Studies Quarterly,* 7 (2), 100-116

Mutetwa, S. (2015) "Baba Jukwa's Facebook page: A possible counter hegemonic space for political transformation in Zimbabwe". *Multilingual Margins*, 2(2), 86-94

Mutsvairo, B. (2016) *Digital Activism in the social media era: Critical reflections on emerging trends in Sub-Saharan Africa*, Switzerland: Palgrave McMillan

Nastasi, B.K. &, Schensul, S.L. (2005*)* "Contributions of qualitative research to the validity of intervention research*"*, *Journal of School Psychology*, 43 (3), 177-195

Ncube, X. (2014, August 27) *Laws on Cards to Curb Cyber Crime*, Retrieved December 09, 2017, from The Zimbabwe Mail: http://www.thezimmail.co.zw

Neumann, W. R. (2002) *Social Research Methods: Qualitative and Quantitative Approaches* (7th ed.), Whitewater: University of Wisconsin

Njanjamangezi, E. (2014, May 16) *90% of Zim Firms Exposed to Cyber Crime*, Retrieved December 09, 2017, from The Zimbabwe Mail: http://www.zimmail.co.zw

Odumesi, J. O. (2006) *Combating the Menace of Cybercrime: The Nigerian Approach (Project)*, Abuja: Department of Sociology

Packard, A. (2010) *Digital media law*, Oxford: Wiley-Blackwell

Paragaz, F. & Lin, T. (2016) *Organisizing and reframing technological determinism*, New Media and Society, 18(8), 1528 – 1546

Parahoo, K. (2006) *Nursing Research: Principles, Processes and Issues* (2nd ed.), Hounds mill: Palgrave Macmillan

Polit, D., & Beck, C. (2004) *Nursing Research: Principles and Methods* (7th ed.), Philadelphia: Lippincott, Williams and Wilkins

POTRAZ. (2017) *Abridged Postal and Telecommunications Sector Performance Report Fourth Quarter 2016*. Retrieved from POTRAZ Web site: http://www.potraz.gov.zw/images/documents/QReports2016/4th_Quarter_Sector_Performance_Report_Final.pdf

Reserve Bank of Zimbabwe. (2015) *Cybercrime in Zimbabwe and Globally*. Retrieved from RBZ Web site: www.rbz.co.zw/assets/cybercrime-globally-and-in-zimbabwe.pdf

Sabao, C., & Chingwaramuse, V. R. (2017) *Citizen Journalism on Facebook and the Challenges of Media Regulation in Zimbabwe: Baba Jukwa.* In Mhiripiri, N.A., & Chari, T. (2017) (eds.) Media law, ethics and policy in the digital age, USA: IGI Global

Samuelson, P. (1998) *Five challenges for regulating the Global Information Society*, Available on http://www.harvardlawreview.org/issues/download/5-99-DEVO.pdf

Savenye, W.C., and Robinson R.S. (2003) *Qualitative Research Issues and Methods: An Introduction for Educational Technologists*, New York: McMillan

Sharma, G. (2017) "Pros and Cons of Different sampling techniques", *International Journal of Applied Research*, 3(7), 749-752

Simon, M. K. (2011) *Dissertation and Scholarly Research: Receipts for Success* (2011 ed.). Saetle: Dissertation Success

Sousa, H., Pinto, M., & Silva, E. (2013) "Digital public sphere: weaknesses and challenges", *Comunicação e Sociedade*, 23 (1), 9 – 12

Squires, C. R. (2002) "Rethinking the Black Public Sphere: An Alternative Vocabulary for Multiple Public Spheres", *Communication Theory*, 12(4), 446-468

Streubert, H. J., & Rinaldi Carpenter, D. (2011) *Qualitative Research in Nursing: Advancing the Humanistic Imperative* (5th ed.), New York: Wolters, Kluwer, Lippincott, Williams and Wilkins

Thornton, A. (2002) *Does Internet Create Democracy?* Available on http://www.zipworld.com.au/~arthonto/thesis_2002_alinta_thornton.doc

UNIDIR. (2013) *The Cyber Index: International Security Trends and Realities*, Geneva: United Nations

Van Dijk, T. A. (1998) *Ideology: A Multidisciplinary Approach*, London: SAGE

Wood, J. T. (1997) *Communication theories in Action*, USA: Wordsworth Publishing Company

Yanshuo, N. (2017) *Cleaning Cyberspace*, China Africa, Vol. 9, July 2017

Yin, R. K. (2011) *Applications of Case Study Research*, London: SAGE

ZDI & MC (2017) *Ordeals in 'the long-walk to Freedom': The State of Internet Governance in Zimbabwe*, Harare: ZDI

ZDI & MC (2018) *The Cybercrime and Cybersecurity Bill: Grave consequences on Internet Freedoms in Zimbabwe! Advocacy Paper*, Harare: ZDI

APPENDICES

INTERVIEW GUIDE

I **Silas Deya,** a final year student at Midlands State University (MSU) studying Media and Society Studies and I am carrying out a research titled **"Investigating the relevance of the introduction of the Cybercrime and Cybersecurity bill in Zimbabwe"**. I kindly ask for your cooperation in assisting me by answering the questions that follows:

1. How important are cyber laws in Zimbabwe in this technological era?
2. Will the country be able to implement such a law and how?
3. Does the law have an impact on freedom of expression as enshrined in the constitution and if so how?
4. Can you briefly explain how the law will protect online users in Zimbabwe?
5. How effective is the current legislation in addressing issues related to cybercrime?
6. Do you think it will be possible to persecute perpetrators of cybercrime, paying attention to user protection of privacy and the use of pseudo names?

QUESTIONNAIRE

I **Silas Deya,** a final year student at Midlands State University (MSU) studying Media and Society Studies and I am carrying out a research titled **"Investigating the relevance of the introduction of the Cybercrime and Cybersecurity bill in Zimbabwe"**. I kindly ask for your cooperation in assisting me by answering the questions that follows:

Gender :

Age :

Educational Qualification :

1. Are you aware of the Cybercrime and Cybersecurity Bill? : Yes [ ] No [ ]
2. Do you think it will help in curbing cybercrimes? : Yes [ ] No [ ]
3. Have you come across any form of cybercrime? : Yes [ ] No [ ]
4. Do you think Zimbabwe is need of such a law? : Yes [ ] No [ ]
5. Please support your answer on the above question :
   ____
   ____
6. How important are cyber laws in Zimbabwe in this technological era? :
   ____
   ____

7. Do you think Zimbabwe will be able to implement such a law? Please support your answer :

   ____

   ____

8. Do you think the bill has an impact on freedom of expression? Support your answer:

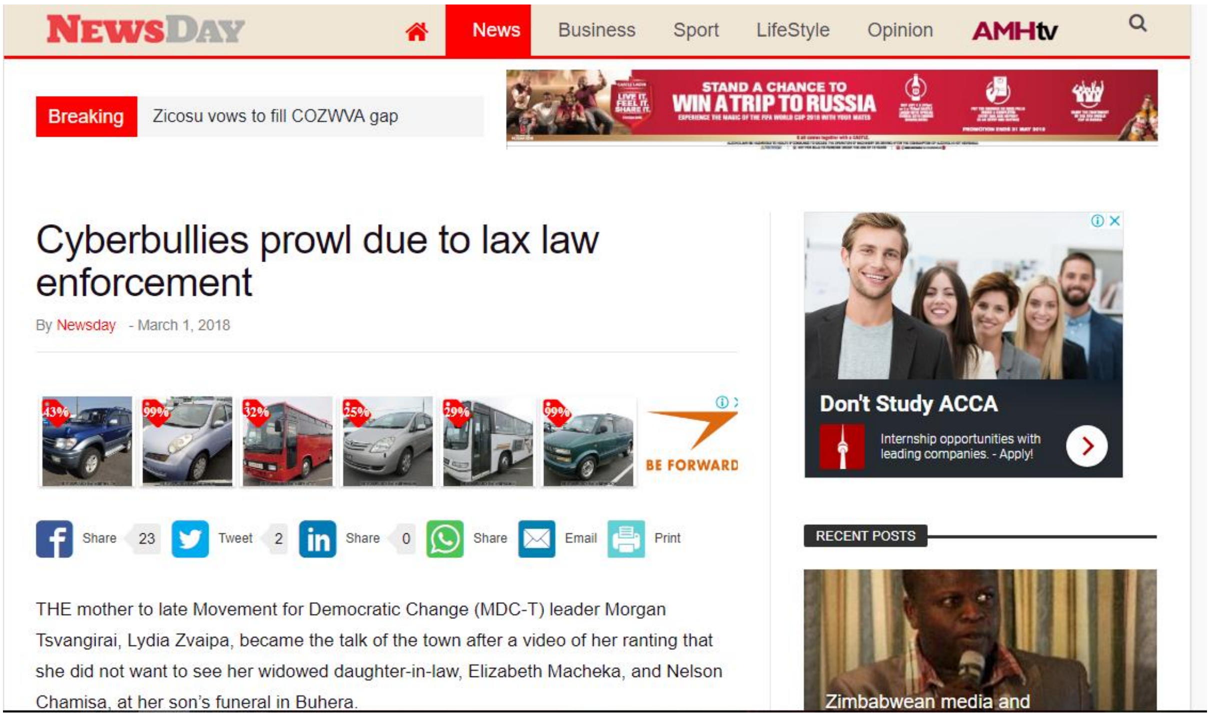
   ____

   ____

9. In your own opinion, how effective is the current legislation in addressing issues related to cybercrime?

____

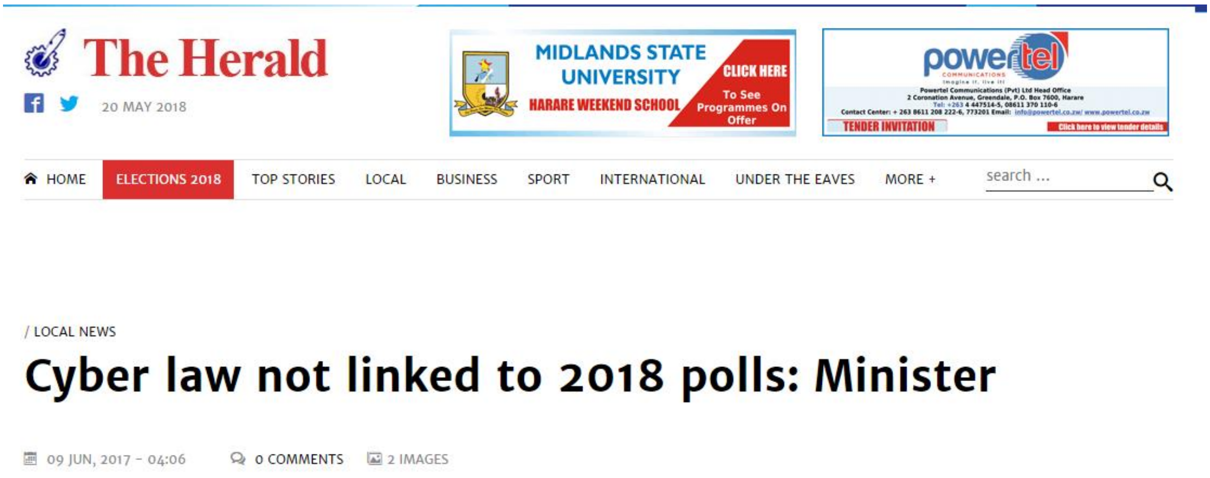
____



Cyberbullies prowl due to lax law enforcement

By Newsday - March 1, 2018

THE mother to late Movement for Democratic Change (MDC-T) leader Morgan Tsvangirai, Lydia Zvaipa, became the talk of the town after a video of her ranting that she did not want to see her widowed daughter-in-law, Elizabeth Macheka, and Nelson Chamisa, at her son's funeral in Buhera.



/ LOCAL NEWS

Cyber law not linked to 2018 polls: Minister

09 JUN, 2017 - 04:06 0 COMMENTS 2 IMAGES