UNIVERSITY OF THE WESTERN CAPE

FACULTY OF LAW

SOUTH AFRICAN-GERMAN CENTRE FOR TRANSNATIONAL CRIMINAL JUSTICE

A CRITICAL EXAMINATION OF THE LAW RELATING TO CYBERCRIME IN UGANDA

by

Timothy Amanya

Student Number: 3875436

Research Paper Submitted in Partial Fulfilment of the Requirements for the LLM

Supervisor: Professor Raymond Koen

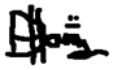
June 2019

TABLE OF CONTENTS

DECLARATION

I, **Amanya Timothy**, declare that **A Critical Examination of the Law Relating to Cybercrime in Uganda** is my own work, that it has not been submitted for any degree or examination in any other University, and that all information from literature I have used or quoted have been duly acknowledged by complete reference.

Student: Timothy Amanya

Signature:  Date: 2 July 2019

Supervisor: Professor Raymond Koen

Signature:…… Date:……..

ACKNOWLEDGMENTS

I am most grateful to GOD, the Lord of Bounty and Majesty for his unfailing mercy.

My humble appreciation to my supervisor, Prof Koen Raymond, for his enormous guidance and ideas that have enabled me to accomplish this research paper.

My sincere appreciation to my parents, relatives, siblings, friends, and classmates for moral, spiritual guidance and encouragement.

I wish also to extend my thanks to German Academic Exchange Service (DAAD) for generously facilitating my studies. A special thanks to Prof Werle, Prof Fernandez, Prof Jamil, Dr Lionel and the staff of the South Africa-Germany Centre for their endless support in the pursuit of this research paper and the LLM course at large.

Möge Gott Sie alle für immer segnen.

ABBREVIATIONS AND ACRONYMS

ACHR	American Convention on Human Rights
ACHPR	African Charter on Human and People's Rights
AUCPDP	African Union Convention on Cyber Security and Personal Data Protection
APA	Anti-Pornography Act
ATA	Anti-Terrorism Act
CMA	Computer Misuse Act
CNRA	Copyright and Neighbouring Rights Act
ECFR	European Charter of Fundamental Rights
ECHR	European Convention on Human Rights
ECOWAS	Economic Community of West African States
ESA	Electronic Signatures Act
ETA	Electronic Transactions Act
NITA-U	National Information Technology Authority Uganda
NITA-U Act	National Information Technology Authority Act
NPPs	Necessary and Proportionate Principles
RICA	Regulation of Interception of Communications Act
SADC	Southern African Development Community
UNHRC	United Nations Human Rights Committee
UN	United Nations
UNGA	United Nations General Assembly
US	United States of America

KEY WORDS

Ambiguities

Basic freedoms

Computer

Crime

Cyber security

Cyber space

Cybercrime

Institutional framework

Investigation

Prosecution

Uganda

CHAPTER ONE

INTRODUCING THE STUDY

1.1 Introduction

Over the last two decades, the world has evolved to an e-era, wherein internet and other digital technologies have become key platforms for the world population, including Ugandans, to enjoy their rights of expression, to associate with other citizens and to engage with leaders.

According to the Uganda Communications Commission, the number of internet users is growing steadily, standing at 13 023 114 as of March 2017 and encompassing 31.3% of the population.[1] However, like other countries across the globe, Uganda is experiencing challenges to the advancement of privacy and freedom of expression online.[2] According to the United Nations, these challenges affect how ordinary citizens, the media, human rights activists and political parties communicate via digital technologies.[3] A key challenge is cybercrime. Ugandans lose colossal sums of money[4] and even human life through cybercrime.

The government of Uganda, in a bid to avert cybercrime, has enhanced cyber security, improved access to information and regulated telecommunications. They include the Anti-Terrorism Act of 2002, the National Information Technology Authority Uganda Act of 2009, the Regulation of Interception of Communications Act of 2010, the Electronic Signatures Act of 2011, the Computer Misuse Act of 2011, the Electronic Transactions Act of 2011, the Uganda Communications Act of 2013, the Anti-Pornography Act of 2014 and the Evidence Act Cap 6 of 1909.

However, these laws contain ambiguous, imprecise, sweeping and confusing provisions that have the potential gravely to affect the enjoyment of rights. Some of these laws negate the full online enjoyment of cyber space. Whereas the government is allowed to limit the

1 Uganda Communications Commission (2017) at 1.
2 The Uganda Police Annual Crime and Road Safety Report (2017) at 10.
3 UNGA Resolution No 64/211 on the Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures (2009) at 1 & 4.
4 Tumushabe & Baryamureba (2005) at 15.

enjoyment of freedoms, the restrictions must be defined narrowly and should conform to the international standards to which Uganda subscribes.[5]

The existing legal cyber framework of Uganda falls short of these standards. The government has acknowledged that it has very weak legislation relating to the cyber space industry.[6] Laws related to intellectual property rights, data security, privacy, data protection and cybercrimes, where they exist, are still in their infancy and enforcement is still low, while other laws are outdated.[7]

Further, the cyber-related laws in existence pose a grievous threat to the rights of the citizenry, with the rights most significantly affected being freedom of expression and the right to privacy. Some of these laws are dedicated cyber laws aimed at the digital environment, whereas other laws are not exclusively directed at the digital environment. This helps to explain the increase in the cybercrime rates in Uganda.[8]

The Ugandan cyber legislation gives the government and its agencies unlimited powers with regard to procuring surveillance equipment, criminalising gadgets and policing internet content. Their powers range from illegally ordering internet service providers to block certain social platforms to signing secret memoranda of understanding among government agencies to share information about internet users and published content in order to enforce the Ugandan cyber legislation. Harassment of online activists by police has been reported also.[9]

Many citizens view the internet as one of the last remaining independent platforms where decent and sound debate can take place and where ideas can be shared without political interference. These developments point to an urgent need to analyse the regulation of the internet in order for citizens to be able to exercise fundamental freedoms, to be empowered

5 UN Special Rapporteur (2011) at 9 & 13.
6 Ministry of Information and Communications Technology (2011) *National Information Security Strategy* (NIIS) at 56.
7 *Uganda vs Dr Aggrey Kiyingi* [2006] UGHC 52 and *Uganda vs Kato Kajubi* [2010] UGCA 73.
8 Mwaita & Owor (2013) at 10.
9 Human Rights Watch (2018) at 504 & 575.

through the internet and to enhance cyber security. It is against this background that a critical analysis of the Ugandan cyber legal framework is proposed.

1.2 The Cybercrime Phenomenon

There is no universally agreed definition of cybercrime. A number of writers use the terms "cybercrime", "computer-related crime", "computer crime" and "high-tech crime" interchangeably. Cybercrime has been defined as "any method of criminality involving use of computers and the internet".[10] This definition points to two main components of cybercrime, namely, a computer and the internet. The term "computer" means:

> an electronic, magnetic, optical, electrochemical, data processing device, and a group of such interconnected or related devices performing logical, arithmetic, and storage functions; and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device or group of such interconnected or related devices.[11]

The term "internet" is defined as:

> a global network wherein devices such as computers, servers, and smart devices are interconnected for data and information exchange. It comprises of public, private, individual and government networks in the domestic and global context, interconnected by a far-reaching array of electronic, wireless, and optical networking technologies.[12]

The evolution of the internet dates back to 1969, following the creation of networking protocols by the Advanced Research Projects Agency Network.[13] The internet protocol address forms the unique identity of a person on the internet. In 2016, the UN General Assembly adopted a non-binding resolution encouraging states parties to promote access to the internet at domestic level. The resolution also recognises internet freedom as a human right.[14]

The concept of cybercrime is applied in relation to three dimensions of criminal activity. The first involves commission of traditional crimes, such as forgery, over electronic

10 Berry (2018) "The Act of Cybercrime", available at https://www.masthead.co.za/newsletter/the-act-of-cybercrime/ (visited 29 May 2018).
11 See Section 1 of the Computer Misuse Act.
12 IP Location, available at https://www.iplocation.net/internet (visited 14 October 2018).
13 Byung-Keun (2005) at 51.
14 UNGA Resolution No 32/L.20 on the Promotion, Protection and Enjoyment of Human Rights on the Internet (2016) paras 12 & 13.

communications networks and information systems. The second dimension covers publication of illegal content, such messages of ethnic hatred, using electronic media. The third concerns crimes exclusive to electronic networks, such as hacking and information system attacks.[15]

Article 28(7) & (12) of the Constitution of Uganda prohibits criminal prosecution of a person under any law unless the act or omission in question constituted a criminal offence at the time of commission or omission, were defined under the law and the punishment was prescribed. The purpose of this provision is to uphold the accused's right to a fair trial which, under Article 44 of the Constitution of Uganda, is non-derogable. The Ugandan Constitutional Court, in *Damian Akankwasa v Uganda*, noted that the test to be applied in petitions relating to Article 28(7) & (12) of the Constitution of Uganda is whether the acts or omissions allegedly performed by an accused person constituted a criminal offence at the time they were performed.[16]

The clause "unless the offence is defined" set out in Article 28(12) of the Constitution is a complex concept in the investigation and prosecution of crime in Uganda. The Supreme Court of Uganda, in *Attorney General v Salvatore Abuki*, attempted to resolve this complexity. The learned justices pointed out that the Court has to determine whether the impugned statute provides sufficient basis for legal debate as to the scope of the conduct prohibited. Further, the Court held that the wording of Article 28(12) does not require that every word or group of words creating a criminal offence should be defined precisely in the English Dictionary.[17]

The principles of *nullum crimen sine lege*[18] and *nulla poena sine lege*[19] curtail efforts to investigate and prosecute computer-related crimes in Uganda. This is because of continuous advances in the tools and techniques of cybercrime commission which facilitate "new crimes" not to be found in the statute books. Section 14(2) of the Judicature Act of 1996 grants jurisdiction to courts to apply natural law, principles of equity, customary law and common law

15 Commission of the European Communities (2007) at 15.
16 Constitutional Reference No 04/11 at 4.
17 Constitutional Appeal No 1 of 1998 at 45.
18 This means that an individual cannot face criminal liability except for an act that was criminalised by law before he or she performed the act.
19 This principle means that a person cannot be punished for doing something that is not prohibited by law.

doctrines insofar as they are consistent with natural law and good conscience.[20] However, this provision is contrary to the constitutional requirement that only offences defined as such in written law be prosecuted and cannot be relied upon in the prosecution of conduct not defined as criminal. Thus, there is a gap in the law as regards combating computer-related crime in Uganda.[21]

1.3 Statement of Problem

The legal framework relating to cybercrime in Uganda is outdated and out of touch with developments in the computer world, and thus largely irrelevant in the circumstances. A case in point is the Evidence Act Cap 6, enacted in 1909. The current circumstances differ from those of 1909 or even of eight years ago, if one considers the Computer Misuse Act of 2011 as an indicator of the dynamism in cyber usage. This dynamism renders the existing laws inappropriate and incapable of achieving the desired standards of cyber security.

The provisions in some of these statutes are a violation of human rights and directed at suppression of opponents of the regime. An example is the switching off of social media and internet access prior to and during presidential elections.[22] The basic freedoms under threat are the right to freedom of expression and the right to privacy, which are laid out in several national[23] and international[24] instruments and treaties which Uganda has signed or ratified. Privacy has been defined as:

> the presumption that individuals should have an area of autonomous development, interaction, and liberty with or without interaction with others, free from state intervention and from excess unsolicited intervention by other uninvited individuals.[25]

20 Judicature Act Cap 13, Laws of Uganda 2000.
21 Amnesty International (2011) at 16.
22 *Amama Mbabazi vs Museveni & Ors* (Presidential Election Petition No 1 of 2016), [2016] UGSC at 3.
23 See Articles 22, 27, 29 & 41 of the 1995 Constitution of the Republic of Uganda (as amended).
24 See Article 19 of the Universal Declaration of Human Rights of 1948.
25 UN Special Rapporteur (2013) para 22.

A number of provisions in the Ugandan cyber-related statutes not only allow for search and seizure of private mobile electronic gadgets and computers,[26] but also do not provide for long-term measures which guarantee the protection of the right to privacy.[27]

There are no provisions in the cyber legal framework for the establishment of an enforcement body or, at minimum, the empowerment of existing units, such as the Uganda Police Force. This omission puts both individuals and the state in peril of cybercrime. This danger has been aggravated by loss of confidence in state entities, which creates a challenge of under-reporting and affects negatively efforts by these organs to combat cybercrime.[28] Individuals with technical cyber knowledge thus continue to steal sensitive information and money through access to online bank accounts or credit card numbers used by online retailers.

In addition, there are numerous juvenile pranks, such as erasing backup files, turning off telephone grids and interfering with traffic systems. These issues were exposed in the case of *Uganda v Garuhanga and Mugerwa*, wherein the accused were charged with embezzlement and false accounting, rather than with computer fraud or computer forgery, regarding the manipulation of computer data resulting in a loss of Ugx3.8 billion to Shell Uganda Limited.[29]

The legal framework contains no requirements or mechanisms for entities using cyber space to instal cyber security tools. This creates a challenge for the detection and prevention of cybercrime by organs such as the Uganda Police Force. The problem was illustrated in the matter involving one Grace Muwanguzi, who was swindled out of a passport and US$500 by a company masquerading as an HIV/AIDs Trainer of Trainers project sponsored by the Ministry of Health and involving officials travelling to Toronto.[30]

In addition, there is the *lacuna* regarding the regulation of the telecommunications services and service providers. The telecommunications industry is operated by private companies, namely, MTN, Airtel and Orange Telecom, all of which tend to pursue profit rather than making efforts to curb computer-related crime. However, there has been no reprimand for

26 See Sections 18 & 19 of the Anti-Terrorism Act 2002.
27 Amnesty International (2011) at 14.
28 Kizza (2003) at 18.
29 [2004] CR 17 Buganda Road Court at 482.
30 Kizza (2003) at 19.

cyber-related crimes attributable to these companies since there is no clear framework establishing liability in such circumstances.

The existing legal framework of Uganda relating to cybercrime is ambiguous and inadequate. The result has been the ineffectiveness of existing entities, such as the Uganda Police Force, leading to an increase in cybercrime involving gross financial losses to both individuals and state entities, and to trampling of human rights, especially of opponents of the regime by the various state agencies. The existing legal framework leaves the victims, present and future, with no relief avenues.

1.4 Objectives of the Study

The study has two core objectives:

- The focal objective of this study is to examine critically the law relating to cybercrime in Uganda in relation to established regional and international standards.
- The study further aims at analysing whether the various cybercrimes in the Ugandan statute book are compatible with freedom of expression and the right to privacy and with full enjoyment of cyber space.

1.5 Research Questions

This research study seeks to answer the following questions:

- What are the nature and form of the cybercrimes in the cyber legal framework of Uganda?
- Are there *lacunae* and ambiguities in the Ugandan cyber legal framework?
- If so, how best may such *lacunae* and ambiguities be resolved?

1.6 Research Hypothesis

This study is guided by the hypothesis that the provisions of Uganda's cyber legal framework fall short of the established international standards, thereby facilitating advanced cyber insecurity and human rights violations.

1.7 Significance of the Study

There are but few writings regarding cybercrime in Uganda, especially critical analyses of the existing legal framework. This study contributes to bridging the gap in knowledge regarding cybercrime legislation in Uganda in relation to regional and international standards.

1.8 Outline of the Remaining Chapters

Chapter Two will discuss the various computer-related crimes enumerated in the various Ugandan statutes.

Chapter Three presents a critical analysis of the Ugandan cyber legal framework in relation to regional and international standards. Reference will be made to various regional and international instruments on the right to privacy and freedom of expression. The chapter forms the gist of the study.

Chapter Four will highlight the general conclusion and findings of the study. Also, it will explore how best the existing gaps in cyber-related law can be closed and how harmony may be created in the national, regional and international legal frameworks.

CHAPTER TWO

COMPUTER-RELATED CRIMES IN UGANDAN STATUTES

2.1 Introduction

This chapter comprises an analysis of the computer-related crimes enumerated in the various Ugandan statutes. The chapter also discusses the nature of computer-related crimes. It analyses these crimes in terms of three categories: offences against the state; offences against confidentiality and integrity; and offences against the person.

2.2 Offences against the State

Crimes committed by use of cyber networks can have a great impact on the security of the state. The intent of the perpetrators, coupled with the impact of a particular act, guides the classification of offences against the state. For the purposes of this paper, these offences will be discussed under two sub-headings: offences against critical national infrastructure and cyber-terrorism offences.

2.2.1 Offences against Key Public Infrastructure

Today the operations of numerous critical sectors are dependent heavily on information and computer technology. It is therefore vital to protect these sectors against cyber-attacks.[1] The Computer Misuse Act (CMA) of 2011 is silent on what amounts to "key public infrastructure". Such a *lacuna* creates an ambiguity in the law and is likely to be used by the state in the oppression and persecution of opposition and the violation of fundamental human rights.[2] Be that as it may, the concept of key public infrastructure encompasses:

> energy (including oil, natural gas, and electric power); banking and finance; transportation (including air, surface, and water transportation); information and

1 US White House (2003) at 22 & 38.

2 Nashif (2017) "Cybercrime Laws as a Weapon against Expression", available at https://www.dw.com/en/cybercrime-laws- as-a-weapon-against-expression/a-41399283 (visited 18 December 2018).

> communications technology networks; water systems; and government and private emergency services.[3]

Cyber-attacks on civilian infrastructure can result in disrupting of power grids, halting of trains, grounding of aircraft and oil pipeline explosions, among others.[4] The substantial increase in these attacks and exposure of the infrastructural networks have propelled governments to recognise the seriousness of the issue. This has resulted in the establishment of mechanisms to enhance cybersecurity in respect of both government and private networks. In this regard, the Anti-Terrorism Act (ATA) of 2002 describes a state or government facility as:

> Any permanent or temporary facility, and conveyance used or occupied by state representatives, government officials, the members of parliament, the judiciary, and employees of a public authority.[5]

The CMA criminalises unauthorised modification of computer material. Section 14(1) of the CMA specifies the requisite intent for this offence as:

> Intent to cause a modification of the contents of any computer and in so doing impairs the operation of any computer or computer programme, hinder access to any programme, and data held in any computer.

Further, the required intent need not be directed at any particular computer, programme or data. A reading of Section 14(4) of the CMA suggests that knowledge about intended modification, whether temporary or permanent, being unauthorised is sufficient to establish the guilt of the perpetrator.

In addition, the CMA provides for an enhanced punishment for offences involving access to protected computers.[6] The punishment is imprisonment for life. This punishment speaks to the gravity of offences against key public infrastructure. Section 20(2)(1) of the CMA describes a protected computer as:

> one used directly in connection with the security, defence or international relations of Uganda; existence or identity of a confidential information source relating to criminal law enforcement; the provision of services directly related to communications infrastructure, banking services, public utilities, and public key

3 Stevens (2016) at 163
4 Stevens (2016) at 163.
5 See Section 2 of the Anti-Terrorism Act.
6 See Section 20(1) of the Computer Misuse Act.

> infrastructure; and protecting public safety, systems relating to essential emergency services such as police, and medical services.

Section 17 of the CMA extends the scope of offences against the state to the offence of unauthorised disclosure of access code. Section 17(2) of the CMA suggests that the perpetrator's knowledge or belief of likely loss, damage or injury to a person or property is a key component in establishing criminal liability for this offence. Sections 21 and 22 of the CMA provide that abetment and attempts to commit the offences under the Act attract, on conviction, punishment for the offence abetted or attempted.

2.2.2 Offences Related to Cyber Terrorism

The concept of cyber terrorism does not have a universally accepted definition. Barry Collin coined the term in the 1970s. He viewed cyber terrorism as a mode in which computer attacks mirrored the effects of ordinary acts of terrorism.[7] However, unlike the use of physical mechanisms, such as suicide bombing, the perpetrators conduct attacks using computer systems. The perpetrators, therefore, need not be present in the territory under attack.[8]

Cyber terrorism also involves actions such as data theft, hacking, and attacks on information systems.[9] The concept of cyber terrorism creates a link between the computer and acts of terrorism. The term "terrorism" has been defined as:

> criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organisation to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism.[10]

Section 13(1)(b) of the CMA criminalises access to a computer with intent to commit or facilitate the commission of an offence. Section 7 of the ATA provides that:

> a person commits an offence of terrorism when, with an intention of influencing the government or intimidating the public or a section of the public and for apolitical,

7 Barry (1997a) at 17.
8 Barry (1997a) at 18.
9 Chawki *et al* (2015) at 39.
10 UN Resolution No 1566 on Threats to International Peace and Security Caused by Terrorist Acts (2004) paras 3 & 4.

> religious, social or economic aim, indiscriminately without due regard to the safety of others or property, seriously interferes with or disrupts an electronic system.

2.3 Offences against Confidentiality, Integrity and the Availability of Computer Data and Systems

2.3.1 Illegal Access to Computer and Information Systems

Illegal access refers to unusual and frequent operations on computer systems without the authorisation of the owner.[11] It usually involves the use of sophisticated software.[12] The terms "unlawful", "illegal" and "unauthorised" are used interchangeably in the different statutes. Access to a computer or computer network without authority or justification of right suffices as illegal access.[13]

The offence of illegal access can take three forms and can be committed severally or jointly, depending on the nature of the act and culpability of the perpetrator. These three forms are:

> unlawful access to a computer system or network; unlawful access to a computer system or network with the intent of obtaining computer data or securing access to any programme, commercial or industrial secrets or confidential information; and unlawful access to a computer programme.[14]

2.3.2 Hacking

The CMA criminalises unauthorised use or interception of a computer service. Section 15(1) of the CMA provides that:

> A person who knowingly secures access to any computer without authority to obtain, directly or indirectly, any computer service commits an offence.

This provision creates two instances of hacking: unauthorised acts relating to computer system and network accessibility; and *ultra vires* acts by the perpetrator.[15]

11 Biegel (2001) at 20.
12 Barry (1997b) at 20 & 24.
13 Wilson (2003) at 3 & 36.
14 Wilson (2003) at 33.
15 Joyner & Lotrionte (2002) at 837 & 839.

The House of Lords, in *R v Bow Street Magistrate; ex parte US Government Allison*,[16] has given guidance on the liability of the perpetrator for *ultra vires* acts relating to computer network and system access. The court held that unauthorised access is established in the following scenarios:

> intentional access to specific data; access was unauthorised by a person entitled to authorise access to that computer or network; possession of knowledge by the perpetrator that the said access to the computer system was unauthorised.[17]

In Attorney General's Reference No 1 of 1991,[18] the court noted that the offence of illegal access to a computer or data is not limited to intentional use of one computer to gain access to another computer. Such an offence can also be committed using a single computer.[19]

2.3.3 Unauthorised Interception

Article 29(2)(a) of the African Union Convention on Cyber Security and Personal Data Protection urges states parties to put in place legislative and regulatory mechanisms to criminalise the fraudulent interception of computers and computer networks during non-public transmission. The Convention, further, urges states parties to criminalise attempt to commit this offence.[20]

Section 15(1)(b) of the CMA criminalises:

> unauthorised interception and unlawful aiding of interception directly or indirectly of a computer or computer network by means of an electro-magnetic, acoustic, mechanical or other device irrespective of similarity.

Section 2 of the CMA provides that interception, in the context of computer function:

> involves listening to or recording a function of a computer and acquiring the substance, meaning of such a function.

2.3.4 Unlawful Data Interference

Section 2 of the CMA describes data as any form of electronic representations of information. Section 8 of the CMA criminalises unauthorised data modification. Criminal liability for this offence is established where the perpetrator modifies or directs modification of computer data

16 [1999] 3 WLR at 620.
17 [1999] ALL ER 1, [2000] 2 AC 216.
18 [1991] NI at 218.
19 Joyner & Lotrionte (2002) at 840.
20 Article 29(2)(b) of the African Union Convention on Cyber Security and Personal Data Protection.

without permission from the rightful owner of the data in question. The authority to interfere with data arises by law or as of right.

This offence involves intentional damaging, deletion, alteration, destruction and suppression of data.[21] The purpose of this enactment is to protect sensitive computer data and programmes from exposure to potential perpetrators. In *Cox v Riley,* the Court held that:

> it is immaterial whether the interference is temporary or permanent. It suffices that the acts committed interrupt or interfere with the lawful use of data by an entitled person, however slight.[22]

2.3.5 Unlawful Interference with an Information System

Section 2 of the CMA describes an information system as a system used for generating, sending, receiving, storing, displaying and processing data messages. This extends to internet and information sharing systems. Section 12(5) of the CMA provides that:

> a person who accesses an information system to constitute a denial of service to legitimate users, whether fully or partially, commits an offence.

The requisite *mens rea* for this offence is established once there is interference with the computer system, irrespective of whether the offence is directed at a particular programme or data in a particular computer.[23]

2.3.6 Misuse of Devices

Section 12(1) of the CMA provides that:

> A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses a device, a computer programme or a component designed primarily to overcome security measures for the protection of data, and performs any of those acts with regard to a passcode or related type of data commits an offence.[24]

21 See Section 9 of the Computer Misuse Act 2011.
22 *Cox v Riley* [1986] 83 Criminal Appeal at 54.
23 Power (2002) at 33.
24 See Section 12(1) of the Computer Misuse Act.

The CMA further criminalises misuse of a computer or computer programme aimed at destroying computer security components, as well as hindering access to computer data and systems.[25]

2.4 Offences Related to Identity Theft

This is a new but rapidly growing mode of cybercrime.[26] The concept of identity theft refers to criminal acts wherein the perpetrator fraudulently obtains and uses another person's identity details.[27] The technique used to obtain the victim's biographical data is known as phishing.[28] The process starts when the perpetrators, masquerading as service providers, send indiscriminate messages to potential victims. The perpetrators identify themselves to their victims as officials in the commonly-used avenues of financial transactions such as PayPal, eBay, Hello Paisa, Mobile Money and MoneyGram.[29] This offence is not defined expressly under the various statutes in Uganda. This lack of precision and clarity creates room for abuse by state agencies under the guise of preventing crime.[30]

The scope of offences related to identity theft extends to the illegal installation of computer software, such as spyware, in the victim's computer system. The aim of the perpetrator in such illegal installations is to keep track of the victim's data: access codes, electronic transaction details, and whereabouts. The perpetrator monitors the flow and operation of data in the devices of the potential victim.[31] This type of crime has been worsened by the invention of botnets, which use remote administration implements, such as malware, against the victim's internet protocol address. These send and return messages, including gathered information, about the victim to the perpetrator in an automated manner.[32]

25 See Section 12(3) of the Computer Misuse Act.
26 Power (2002) at 30.
27 Power (2002) at 53.
28 Lynch (2014) at 262.
29 Chawki *et al* (2015) at 45.
30 Power (2002) at 29 & 33.
31 Barry (1997b) at 20.
32 Jakobsson & Myers (2006) at 215.

2.5 Computer-Related Economic Offences

The purpose of criminalising computer-related economic offences, such as fraud and forgery, is to protect people's interests in property, financial assets and document authenticity.[33] The AU Convention on Cyber Security and Personal Data Protection urges member states to:

> establish key legislative and regulatory mechanisms to criminalise fraudulent procurement committed with the aid of a computer or cyber space.[34]

Computer fraud may take the form of modification or alteration of computerised data for personal or third-party gain. According to the Electronic Transactions Act (ETA) of 2011, unlawful alteration extends to acts of unauthorised interference with the use of a given computer system.[35]

2.5.1 Electronic Fraud

Electronic fraud refers to:

> acts involving computer manipulation, by whatever technique, with a purpose of dishonestly obtaining money, property, some other form of advantage of value, and causing loss. Further, fraud includes making false statements to a person upon which said person relies to make a decision, resulting in damage to the innocent party.[36]

Section 19(1) of the CMA criminalises electronic fraud. A reading of Section 19(2) of the CMA suggests that electronic fraud involves:

> deception performed deliberately with a purpose of securing an unlawful, and unfair gain wherein part of the communication facilitating commission of the offence is sent through a cyber system.[37]

The fraud may be committed entirely within the computer network. The CMA imposes a fine not exceeding 360 currency points or imprisonment not exceeding 15 years or both upon a conviction for this offence.[38]

---

33 Glyn (1983) at 84.
34 Article 8 of the AU Convention on Cyber Security and Personal Data Protection.
35 See Section 29(d) of the Electronic Transactions Act.
36 Bainbridge (2007) at 280.
37 See Section 19(2) of the Computer Misuse Act.
38 See Section 19 of the Computer Misuse Act.

Section 26(3) of the ETA extends the scope of fraud to that committed often by companies, such as telecommunication companies, which charge customers for unsolicited messages and calls. This offence involves a person sending messages not sanctioned by the receiver. The punishment for this offence is a fine of 152 currency points or imprisonment not exceeding five years or both.[39] The purpose of this provision is to curtail fraud primarily perpetrated by corporations charging telecommunication subscribers for unsolicited texts.[40]

2.6 Offences Relating to Intellectual Property Rights

Section 5(1)(e) of the Copyright and Neighbouring Rights Act (CNRA) of 2006 identifies computer programmes, electronic data banks and other accompanying materials as items eligible for copyright. Section 13(6) protects the economic rights of authors of computer programmes for a period of 50 years from the date of the programme being made available to the public.

Section 46 of the CNRA provides for the various forms of copyright infringement. It encompasses unlawful dealing with works or performances of an individual: without authorisation by the *bona fide* owner of the rights; and in excess of or contrary to the nature of the authorisation granted to a person by the entitled person.[41] The authorisation to use or alter a copyright may be obtained through transfer, licensing, assignment and any other form recognised under the laws of Uganda. This authorisation ought to be express and clear.[42] This implies that unlawful usage of a person's copyrightable material through a cyber network constitutes a computer-related offence.

Further, Section 47(7)(a)-(b) of the CNRA criminalises illegal removal or alteration of any electronic moral rights information. The scope of this offence extends to availing performances, copies of a sound recordings, and audio-visual fixation to the public with prior knowledge by the perpetrator of its unauthorised alteration.[43]

---

39 See Section 26(4) of the Electronic Transactions Act.
40 Sofaer & Seymour (2001) at 89.
41 See Section 47 of the Copyright and Neighbouring Rights Act.
42 See Section 46(1) of the Copyright and Neighbouring Rights Act.
43 See Section 47(c) of the Copyright and Neighbouring Rights Act.

In *R v Gilham*, the court set out the elements of computer-related copyright offences in the following terms:

> that the computer software is or includes copyright works within the meaning of the provisions of the intellectual property statute; that the copyright work was copied by the offender; that such copying is of the whole or a substantial part of a copyright work; that the copies of the copyright work or works created by or with the licence of the owner of the copyright include effective technological measures within the designed to protect those copyright works; that in the course of a business the defendant sold or let for hire a device, product or component which was primarily designed, produced, or adapted for the purpose of enabling or facilitating the circumvention of those technological measures. It bears noting that this issue does not depend on the intention of the defendant who is not responsible for the design, production, and adaptation of the device is irrelevant. His intention is irrelevant.[44]

2.7 Offence of Cybersquatting

Cybersquatting has been defined as:

> Illegal acts of registering, trafficking in and using an internet domain name with a wrongful intent to profit from the goodwill of a trademark or company belonging to another person.[45]

Further, cybersquatting involves registration by the perpetrator of a domain name containing common words or an existing trademark or business name of a potential victim.[46] The perpetrator uses the registered domain either to redirect business to himself or sell the domain at an inflated price; or he may use it to sell products or services which appear to have connections to the trademark or business in question. The victim is oftentimes unaware of the transaction at its initial stages because of the complexity of this offence and a lack of knowledge about computer-related crime.[47]

2.8 Offences against the Person

These are offences that have a direct impact on individuals.[48] They include child pornography, cyber stalking, and cyber harassment.

---

44 [2009] All ER at 89.
45 Kilian (2000) at 25.
46 Hansen-Young (2005) at 14.
47 Chawki *et al* (2015) at 54.
48 Kilian (2000) at 34.

2.8.1 Offence of Child Pornography

A child means a person below the age of 18 years.[49] The avenues often used by perpetrators in the commission of this offence include websites, blogs, discussion forums and social media platforms, such as WhatsApp, Facebook and Instagram.[50]

Section 23 of the CMA criminalises child pornography**.** The offence of child pornography involves:

> production of child pornography for the purposes of its distribution through a computer; offering or making available child pornography through a computer; distributing or transmitting child pornography through a computer; procuring child pornography through a computer for himself or herself or another person; and unlawful possession of child pornography on a computer.[51]

Further, Section 23(1)(b) of the CMA makes it an offence to make available pornographic materials to a child.

Section 23(3) (a)-(c) of the CMA describes child pornographic materials to mean materials that portray:

> a child engaged in sexually suggestive or explicit conduct; a person appearing to be a child engaged in sexually suggestive or explicit conduct; and realistic images representing children engaged in sexually suggestive or explicit conduct.

Section 23(4) of the CMA imposes a punishment of a 360-currency point fine or a 15-year jail sentence or both on a perpetrator convicted of the offence of child pornography.

The Anti-Pornography Act (APA) of 2014 also criminalises acts of child pornography.[52] It provides that a person commits an offence of child pornography by:

> producing, participating in the production of, trafficking in, publishing, broadcasting, procuring, importing, and exporting or in any way abetting pornography depicting images of children.

The Act provides for a fine of 750 currency points or imprisonment not exceeding 15 years or both as the punishment for said offence. Section 14(2) of the APA stipulates that, in

---

49 See Section 2 of the Anti-Pornography Act 2014 & Article 2 of the African Charter on the Rights and Welfare of the Child.

50 Coetzee (2013) at 752.

51 See Section 23(1) of the Computer Misuse Act.

52 See Section 14 of the Anti-Pornography Act.

determining liability for the offence of child pornography, the definition contained in section 2 of the same statute should be considered.

2.8.2 Offence of Offensive Communication

The offence of offensive communication covers acts relating to possession of written material or recorded pictures or sounds which are threatening, insulting or abusive, with the purpose of using them against the integrity or confidentiality of an individual. This negative data then is channelled through a computer network to a third-party in order to disgrace the victim. In worst-case scenarios, such as blackmail, the perpetrator may seek a ransom from the victim in order to contain the abuse.[53]

Article 29(3)(1)(f)-(h) of the African Union Convention urges states parties to criminalise acts of offensive communication. The African Union Convention provides that:

> Acts of offensive communication extend to threats and insults channelled through a computer systems against a person owing to the person's membership of a particular group distinguished by race, colour, descent, national or ethnic origin or religion where such membership serves as a pretext for any of these factors, or against a group of persons which is distinguished by any of the characteristics.[54]

These acts involve wilful and repeated use of electronic media to disrupt peace, and are a hindrance to the enjoyment of the right to privacy by the victim, given that the intent of perpetrator is to use an illegitimate communication to cause grief to the victim. The scope of the offence extends to attempts by the perpetrator to commit it.[55] This offence is treated as a misdemeanour and upon conviction attracts a fine of 24 currency points.[56]

2.8.3 Offence of Cyber Harassment

This is provided for under section 24 of the CMA. It involves:

> making obscene, indecent, lewd, and lascivious requests, suggestions, and proposals; threats calculated at inflicting injury or physical harm to a person or property; and a person authorising use of electronic devices with knowledge that

53 Chawki *et al* (2015) at 40.
54 See Article 29(3)(1)(g) of the African Union Convention on Cyber Security and Personal Data Protection.
55 See Section 25 of the Computer Misuse Act.
56 See Section 25(2) of the Computer Misuse Act.

device in question is to be used in the commission of the acts in section 24 of the Act.

The CMA provides for a fine of 72 currency points or imprisonment for three years or both as punishment for this offence.[57]

2.8.4 Offence of Cyber Stalking

According to Mishler, this offence involves continuous use of cyber space and electronic devices to intimidate or annoy a person or group of persons.[58] However, there are numerous acts associated with cyber stalking. Such acts include threats, false accusations, insults, network attacks, unlawful spying, impersonation, harassment, and physical assaults upon the victim. The establishment of a causal link between cyber space and any of such acts points to the offence of cyber stalking.[59]

Section 26 of the CMA criminalises frequent malicious and wilful cyber harassment of a person. Further, a reading of the section suggests that threatening persons with an intent to put them under reasonable fear for their personal safety or the safety of their immediate family members suffices as cyber stalking.[60] The punishment upon conviction for the offence of cyber stalking is a fine not exceeding 120 currency points or imprisonment not exceeding five years or both.[61]

2.9 Conclusion

This chapter has discussed the various cybercrimes listed under the various Ugandan statutes. These involve offences against the state, individual confidentiality, integrity and reputation, and cyber-related economic offences. However, key concepts in the investigation and prosecution of these offences remain undefined, such as “key public infrastructure” and “public data”. The chapter reveals that certain crimes are not defined clearly under the statutes. These

57 See Section 24(2) of the Computer Misuse Act.
58 Mishler (2000) at 116.
59 Beagle (2011) at 457.
60 See Section 26(1) of the Computer Misuse Act.
61 See Section 26(2) of the Computer Misuse Act.

ambiguities in the law carry a risk of being utilised by state authorities to violate fundamental human rights.

CHAPTER THREE

UGANDAN CYBRECRIME LAW IN TRANSNATIONAL PERSPECTIVE

3.1 Introduction

This chapter begins with a discussion of the international human rights standards relating to the right to privacy and freedom of expression. This is done by analysing various provisions in regional and international statutes, treaties, declarations and conventions. The chapter, further, sets out an analysis of the legal restrictions affecting the free use of cyber space.

It bears noting that the international human rights standards in question are mostly soft law. Therefore, they are largely non-binding upon states parties. They take the form of recommendations and guidelines. The right to privacy differs from data protection rights, although they overlap. Personal data is defined as any information capable of being identified with a natural person. The distinction between the right to privacy and data protection rights is that not all information relating to an identifiable person falls within the scope of privacy. Data protection rights cover a wider scope compared to privacy.

3.2 International Covenant on Civil and Political Rights

The International Covenant on Civil and Political Rights (ICCPR) came into force on 23 March 1976 and was ratified by Uganda in 1995. It is a multilateral treaty. Article 17 of the ICCPR prohibits arbitrary or unlawful interference with an individual's privacy, family, home or correspondence and unlawful attacks upon a person's honour and reputation.[1] Further, the Covenant provides for freedom of expression,[2] which includes an individual's ability to seek, receive and impart information and ideas of all kinds, regardless of frontiers, whether orally, in writing or in print, in the form of art or through any other media of his choice.[3]

1 See Article 17(1) of the ICCPR.
2 See Article 19 of the ICCPR.
3 See Article 19(2) of the ICCPR.

The UN Human Rights Committee (UNHRC) asserts that freedom of expression extends to internet and computer-based forms of expression.[4] The rationale for this assertion is to cater for the dynamics in information and communication technology.[5] The Constitution of the Republic of Uganda guarantees the right to privacy[6] and freedom of expression.[7] The constitutional guarantees of these rights are appealing in theory, but the practice reveals persistent non-observance. However, enjoyment of this right is subject to limitations in the form of protection of the public interest and enjoyment of fundamental human rights by other persons.[8] The Constitution, however, does not define "public interest".

The ICCPR obligates states parties to establish and maintain measures to secure media independence and freedom of access to electronic and print media. The right to access information requires states parties to set up mechanisms of access to data in the custody of state agencies.[9] The dates of production, form of data storage and source, extra-judicial arrests, torture, murder, and threats to human life should not be used as a limitation upon access to public information. However, Article 19(3) of the Covenant empowers states parties to activate limitations where enjoyment of cyber freedoms poses a threat to the national interest and the restrictions adopted are essential to protect other people's rights, public order, public health and the values of society. According to the ICCPR, the restrictions must be proportionate and prescribed in law.

According to the UNHRC, states parties should ensure that their law enforcement agencies respect and uphold the freedom of expression. These measures should be published and accessible to the public.[10] Further, restrictions on the use of search engines, websites and social media should accord with Article 19(3) of the Covenant.

4 UN Special Rapporteur (2013) para 22.
5 Sobotta & Kokkot (2013) at 225.
6 See Article 27 of the 1995 Constitution of Uganda.
7 See Article 26 of the 1995 Constitution of Uganda.
8 See Article 43 of the 1995 Constitution of Uganda.
9 See Article 19(2) of the ICCPR.
10 UN Special Rapporteur (2011) paras 584 & 585.

The UNHRC submits that states parties should ensure that their counter-terrorism measures are compatible with the Covenant.[11] Therefore, terrorism-related crimes, such as encouraging terrorism, justifying terrorism and praising terrorism, should be written and described clearly under the law of the state party. The rationale is to protect individuals from political persecution under the guise of anti-terrorism campaigns. In addition, media houses and journalists should not be restricted unjustifiably and penalised for acts in discharge of lawful duties.[12]

The Covenant prohibits unlawful surveilling, wire-tapping and interception of communication lines.[13] It obligates states parties to establish measures to prevent third parties from illegally accessing information about the private life of individuals. Therefore, states parties are required to legislate for the protection of personal data held by private and public entities, irrespective of the nature of the device. Individuals must be able to liaise with the technology firms regarding the maintenance and security of their data. This means that individuals should be allowed to make alterations to their personal data in the custody of agencies.[14]

3.3 Universal Declaration of Human Rights

The UN General Assembly adopted the Universal Declaration of Human Rights (UDHR) in 1948. The Declaration prohibits unlawful interference with a person's home, family, privacy, honour and correspondence or attacks upon an individual's reputation.[15] This means that states parties have to establish measures to protect and uphold these rights. The UDHR further stipulates that every person has a right to freedom of expression and opinion.[16] The freedom of opinion involves seeking, receiving and imparting information and ideologies without unlawful interference.

11 UNHRC General Comment 16 to Article 17 of the ICCPR (1988) paras 6, 7 & 8.
12 Sobotta & Kokkot (2013) at 224 & 226.
13 See Article 17 of the ICCPR.
14 UN Special Rapporteur (2011) para 588.
15 See Article 12 of the UDHR.
16 See Article 19 of the UDHR.

3.4 European Convention on Human Rights

The European Convention on Human Rights (ECHR) is the major human rights instrument in the European region. It is not binding on Uganda. However, the European region largely has upheld the protection of human rights and conforms to international standards. Therefore, the legal standards in the region can be used to shape Uganda's human rights standards. Article 8 of the Convention provides for respect for a person's privacy and protection of freedom of expression. The freedom of expression involves protection of freedom of opinion, regardless of frontiers.[17] These rights can be subject to restrictions only in terms of written law.

Further, the restrictions must be in accordance with established democratic principles, for public safety and necessary for the protection of health, morals, state interests and other people's rights.[18] According to the ECHR, restrictions may be invoked to prevent disclosure of confidential information and crime, and maintenance of impartiality in state organs.[19] The European Court of Human Rights, in *Dubská and Krejzová v Czech Republic,* has given guidance on the test for activating public interest as a restriction. The Court, *inter alia*, noted that:

> Therefore, there has to be a social interest proportionate to the legitimate aim sought by the government in order to invoke interference with a person's communication and devices.[20]

3.5 Charter of Fundamental Rights of the European Union

The European Charter of Fundamental Rights (ECFR) came into force in 2009. The ECFR is not binding on Uganda. However, like the ECHR, the ECFR largely conforms to the standards set by the International Covenant on Civil and Political Rights. For this reason, coupled with the standard of implementation of the ECFR, it is worth borrowing a leaf from it in the context of human rights protection in Uganda. It should be noted that in cases of corresponding provisions in the ECFR and the ECHR, the rights in question are assumed to be similar.[21]

Article 7 of the Charter provides protection of the right to respect for individuals, families, homes and communications. The ECFR, further, provides for protection of a person's

17 See Article 8(1) of the ECHR.
18 See Article 8(2) of the ECHR.
19 See Article 10(2) of the ECHR.
20 Applications 28859/11 and 28473/12 paras 5 & 6.
21 See Article 52(3) of the ECFR.

private data.[22] In addition, limitations to this right should be exercised fairly. The Charter provides that the consent of the person in question should be obtained through legitimate procedures. This right extends to one's ability to access information concerning one in another person's custody and the right to rectify the data in question.[23] Article 8(3) of the ECFR calls upon states parties to establish an autonomous body charged with ensuring compliance of their data protection rules with the provisions of the ECFR.

In 2004, the European Court of Justice declared invalid Directive 2006/24/EC for containing provisions interfering with the observance, upholding and protection of the right to respect, privacy and protection of personal information beyond the prescribed standard of restriction. The Court held that the European Union Legislature, in endorsing the Directive, acted *ultra vires*.[24]

Article 11 of the Charter provides that every individual has a right to freedom of expression. This right extends to freedom of opinion and freedom to access and share data and opinions without state or private interference, regardless of frontiers.[25] Article 11(2) urges states parties to respect media pluralism and freedoms. Thus, any limitations on enjoyments of the rights and freedoms listed in the ECFR must be prescribed by law and consider the importance of such rights and freedoms.[26] Limitations should be activated in accordance with the recognised interests of the European Union. The limitations should be invoked as a last resort against cyber misuse.

3.6 American Convention on Human Rights

The American Convention on Human Rights (ACHR) is not binding on Uganda but is an example of an instrument largely compliant with international human rights protection standards. The Convention prohibits unlawful interference with a person's communications, information,

22 See Article 8 of the ECFR.
23 See Article 8(2) of the ECFR.
24 Cases C-293/12 & C-594/12.
25 See Article 11(1) of the ECFR.
26 See Article 52 of the ECFR.

devices, data, family and property. This protection extends to illegal attacks on a person's character.[27]

> Article 13(1) of the ACHR provides that freedom of expression:
>
> involves freedom to access, seek, distribute, and impart ideologies and information irrespective of frontiers and form of media used by the person.[28]

The common typologies are electronic and print media. The Convention suggests that freedom of expression ought not to be subject to restrictions.[29] States parties are prohibited from activating indirect control measures, such as suspension of media, that limit enjoyment of these rights and freedoms.[30] However, states parties can subject the freedom to liability which should be written clearly and described under the law.[31]

3.7 African Charter on Human and Peoples' Rights

Uganda ratified the African Charter on Human and People's Rights (ACHPR) in 1986. It is binding on Uganda. The Charter has no express provisions on the right to privacy. However, the ACHPR provides for freedom of expression.[32] Article 8(1) of the Charter states that this freedom includes the right to receive and disseminate information in accordance with the prescribed law of the state party.

3.8 International Principles on the Application of Human Rights to Communications Surveillance

These Principles are drawn from reports and opinions of civil society, industrialists, international human rights law experts, distinguished academicians, and international best practices. They are referred to also as the Necessary and Proportionate Principles (NPPs). The NPPs attempt to explain the current trends in international human rights application, particularly regarding information and cyber systems. Therefore, states parties ought to adopt

27 UN Special Rapporteur (2011) para 586.
28 See Article 13(1) of the ACHR.
29 See Article 13(2) of the ACHR.
30 See Article 13(1) of the ACHR.
31 See Article 13(4) of the ACHR.
32 See Article 9 of the ACPHR.

and practise the Principles in order to realise an effective human rights protection system. However, the NPPs are not legally binding.[33]

The principles of proportionality, transparency, necessity, adequacy, communication integrity, legitimacy, transnational co-operation and legality are vital in the activation of the NPPs. The principle of proportionality means communication-related decisions should be made in consideration of the sensitivity of the data accessed and likely damage to be caused by such release. With regard to adequacy, communication restrictions should be legitimate and appropriate to the identified purpose.[34]

States parties are required to establish communication surveillance mechanisms and procedures that are protective of human rights. The process of communication surveillance involves operations such as crime investigation, enhancement of state security networks, and protection of other people's rights. In activating communication surveillance, state agencies should ensure that:

> the device or data in question is relevant and necessary in investigation and prosecution of a particular crime; there is overwhelming evidence of a crime being committed or being about to be committed; all less aggressive techniques have been exhausted or will be futile; accessibility to data will be confined to that relevant in the investigation and prosecution of a heinous crime or threat to public interest; a person's data collected will be protected from third parties; this involves complete destruction of the said data once the criminal proceedings end; the information will only be used for the purpose brought to the person's notice; the proposed techniques do not restrict the individual's enjoyment of fundamental rights and freedoms; and the agencies conducting the surveillance are autonomous in their operations.[35]

3.9 Joint Declaration on Freedom of Expression and the Internet

This Declaration was adopted in 2011. It is authored by Special Rapporteurs for Freedom of Expression across the globe. The Declaration discusses issues related to maintenance and protection of the right to privacy and freedom of opinion and expression, with a focus on Article 19 of the International Covenant on Civil and Political Rights. The Declaration lists guidelines essential to protecting internet freedoms. These include:

33 UN Special Rapporteur (2013) paras 23 & 24.
34 Principle III of the NPPs.
35 LaRue *et al* (2014) at 52.

> absolute protection of third parties with respect to data produced by technical internet providers; regulatory systems for other technologies should not be applied to cyber freedoms; States Parties to apply 'real and substantial connection' and 'substantial harm' tests in ascertaining criminal and civil jurisdiction in computer-related offences; States Parties called upon to formulate and implement strategies aimed at promoting access to and use of internet; transparency in communication control mechanisms and non-discriminatory treatment of cyber networks and systems; and cyber filtering systems such as blocking access to particular websites should only be permitted in cases of protection of other peoples' fundamental human rights. For example, protecting children from pornography and ideological disorientation.[36]

These guidelines, though not legally binding on Uganda, could help in shaping a pro-human rights legal, policy and institutional framework in the country.

3.10 African Declaration on Internet Rights and Freedoms

This Declaration was launched in 2014, with the purpose of establishing and developing regional standards regarding internet and computer freedoms.[37] Further, the Declaration echoes the need for concerted efforts of all stakeholders, including civil society, regional and international organisations, to ensure enjoyment of the right to privacy and freedom of expression.[38] The Declaration suggests key principles to be adopted by states parties to realise the desired standards of enjoyment of internet freedom. These include:

(a) **Openness.** This involves creating and enhancing favourable avenues for exchange of ideas and information. This is achieved by creating an integrated system that promotes freedom of opinion and expression, cultural diversity and media pluralism. States parties also have to support cyber-related innovativeness and invention.[39]

(b) **Internet Access and Affordability.** This includes states parties making the internet affordable and available to the citizenry without discrimination as to sex, race, social origin and any other status. The justification for this principle is its being a necessity for the realisation of human development. This is because the internet plays a key role in

36 UN Special Rapporteur (2012) para 33.
37 See Para 5 of the Preamble to the Declaration.
38 See Paras 6 & 7 of the Preamble to the Declaration.
39 Key Principle 1 of the Declaration.

the enjoyment of other fundamental human rights, such as the right to education, assembly, and socio-cultural participation.[40]

(c) **Freedom of expression.** This involves freedom to access and impart ideas or information of all forms through cyber space, regardless of frontiers. This freedom should be subject only to restrictions that are necessary and proportionate to the state party's legitimate purpose.[41]

(d) **Right to information.** The principle suggests that information related to scientific and social research should be made available to persons interested in accessing it.[42]

The other principles highlighted in the Declaration are: freedom of association, cultural diversity, the right to access knowledge, cyber security, protecting internet freedoms of marginalised groups, the right to due process, gender equality and democratic cyber network management.[43]

States parties and non-state entities, such as civil society, academic and research institutions, media houses, and information and technology corporations, can adopt the Declaration and use it to shape and enhance internet freedom protection standards in the region. In addition, the Declaration obligates states parties to establish safeguards against violations of the right to privacy and freedom of opinion, and ensure that the telecommunications and cyber sectors are facilitated, transparent and independent in discharging their duties.[44]

The above discussion (§3.2 to §3.10) presents the established best practices and international and regional standards related to protecting enjoyment of internet freedoms. These are drawn from regional and international instruments, reports by UN Special Rapporteurs and treaties. There appears to be a common ground in requiring states parties to promote the enjoyment of internet freedom by everyone. The discourse points to the nature and conditions attached to potential restrictions upon the enjoyment of these rights and

40 Key Principle 2 of the Declaration.
41 Key Principle 3 of the Declaration.
42 Key Principe 4 of the Declaration.
43 Key Principles 5,6,7,8,9,10 & 12 of the Declaration.
44 www.africainternetrights.org (visited 2 May 2019).

freedoms. The analysis below involves a critique of the existing cyber-related legal framework of Uganda against the regional and international standards.

3.11 Anti-Terrorism Act

In 2002, as a response to global calls to combat terrorism, the Anti-Terrorism Act (ATA) was enacted in Uganda. The ATA provides for the death sentence as punishment for persons who establish, run or support terrorist institutions, through imparting ideologies to others, raising funds for terrorism or mobilising persons for terrorist operations.[45] The Act indirectly permits interference with a person's private data, family, life and correspondences upon suspicion of the person committing or planning to commit terrorism.

The UN Special Rapporteur on the Right to Privacy asserts that under international human rights law states are required to criminalise incitement of terrorism at the domestic level.[46] However, such criminal provisions should comply with the regional and international standards. The restrictions should be in pursuance of a legitimate aim and respect for the principles of proportionality and necessity.

The Special Rapporteur proposes further that the desire to protect state security and implement counter-terrorism measures cannot be used to justify a violation of the right to privacy and freedom of expression. The Special Rapporteur considers that restrictions upon the enjoyment of these rights can be activated only when:

> the information disseminated is calculated at inciting imminent violence; the information in question is likely to incite such violence; and there is a substantial immediate and direct nexus between the expression and the possibility or actual occurrence of such violence.[47]

The ATA is silent on the definition of promotion of terrorism. Further, the ATA does not provide for what amounts to pro-terrorism material. It is right to hold that this law is ambiguous, unpredictable and thus falls short of the established international standards of transparency and predictability of the law. This *lacuna* creates an enforcement dilemma and makes citizens

45 See Section 9(1) & (2) of the ATA.
46 UN Special Rapporteur (2013) para 81.
47 UN Special Rapporteur (2012) para 73.

susceptible to unnecessary surveillance. In addition, the UN Human Rights Committee, in a commentary on Article 19 of the ICCPR, postulates that states parties should protect persons from all forms of attack arising from their expressions, opinions and ideologies. These attacks include torture, extra-judicial arrests, and threats to one's life, property and family.[48]

Section 9(2) of the ATA provides for the death sentence as punishment for the publication or dissemination of pro-terrorism material. The death sentence as a punishment for a crime defined ambiguously in the ATA is an attack upon the enjoyment of internet freedoms enshrined in the various international instruments that Uganda has signed or ratified. The punishment is also a violation of international human rights, particularly the right to life and protection against degrading treatment. In addition, arbitrary use of criminal sanctions to curtail legitimate expression of opinions and ideologies is a grave limitation upon the enjoyment of that freedom.

Part VII of the ATA covers communication surveillance. Section 18 authorises the Minister of Internal Affairs to designate officers with rights to conduct surveillance on an individual, group or institution suspected of committing any of the offences in the ATA. The surveillance is conducted on the person's devices, electronic media platforms and correspondence. According to the ATA, communication surveillance may be conducted to:

> safeguard state interest; prevent violation of fundamental human rights and freedoms of other persons through acts of terrorism; detect and prevent commission of any offence under the Act; and protect the state economy from terrorism.[49]

Section 20 of the ATA prescribes a two-year jail term for a person who obstructs an officer conducting surveillance under Part VII. The Act is silent on the procedure to be followed by the Minister in designating the officials to conduct communication surveillance. Such gaps in the law serve only to create a suitable environment for abuse of power by the designated persons, to the detriment of the citizenry. The Act is also bereft of impartial, transparent and autonomous checks regarding such arbitrary actions.

48 UN Special Rapporteur (2012) paras 77 & 78.
49 See Sections 18 & 19 of the ATA.

The failure of the ATA to conform to the established regional and international standards has been summarised by Amnesty International in the following terms:

> the overly broad definitions of "terrorism", "aiding and abetting" terrorism and the fact that "promoting terrorism" is not defined under the Uganda Anti-Terrorism Act are to be viewed as inhibiting media pluralism and criminalising legitimate media coverage. Even the interception powers of the authorised officers are criticised as they could make it possible to intercept communications between journalists and their sources.[50]

It is submitted that the Anti-Terrorism Act contains provisions that are in violation of or create an environment for the violation of people's fundamental rights, particularly cyber freedoms. The Act falls short of the regional and international standards regarding protection of the right to privacy and freedom of expression.

3.12 National Information Technology Authority Act

The National Information Technology Authority Act (NITA-U Act) establishes and empowers the National Information Technology Authority (NITA-U). The Authority is mandated to design and enforce policies and strategies necessary for promoting a vibrant technological system in the country.[51] Section 5 of the Act attempts to structure broad functions, and makes public servants susceptible to communication and information surveillance.

Section 5(3) of the NITA-U Act mandates the Authority to co-ordinate, supervise and monitor the use of information technology systems. However, the Act is silent on the scope of the supervision and monitoring to be done by NITA-U. The Act leaves the concept of "use of information technology systems" unexplained, making this provision unclear and ambiguous. The provision creates space for a default interpretation of the concept of technological utility which expands the supervisory and monitory powers of the Authority. This interpretation easily could subject persons to illegal cyber attacks and unlawful interceptions of personal data.

The Act also mandates NITA-U to regulate and enforce standards for information technology hardware and software equipment procurement in all government sectors, agencies

50 Amnesty International (2011) at 14.
51 See Section 3(2) of the NITA-U Act.

and parastatals.[52] This mandate can be exploited to instal spy software and filters in the state devices. These software programmes conduct illegal surveillance on civil servants by relaying reports on their website visits and correspondence. NITA-U also is obligated to create, design and maintain a national data system.[53] The statute is silent on the nature, mode and form of data to be stored in the national database. The origin, maintenance and procedures of obtaining said data equally are unexplained in the Act. This gap creates room for illegal interception under the guise of collecting data for the national database, which violates the right to privacy. Further, the nature of the database is unclear. This makes people's data susceptible to unlawful access by third parties.

The Act obligates NITA-U to establish, maintain and regulate aspects of technological planning, organisation, delivery, support systems, disposal, database security, policy implementation and disposal systems.[54] Section 5 of the Act grants wide undefined powers to NITA-U to establish guidelines and regulations regarding the utility of information technology systems. The Act does not explain what the regulation procedures involve, thereby creating opportunities for violation of the right to privacy through unnecessary interceptions of and interference with personal data and devices.

Part V of the Act regulates information technology surveys and the powers of NITA-U. Section 2 states that technology surveys involve:

> the review, examination, inquiry, information gathering and analysis of ICT-related materials or data.

The Minister of Information and Computer Technology, with the consent of the board established under the Act, is authorised to give directions for conducting a survey in the public and private sectors.[55] According to Section 7(2) of the Act, the board members are appointed by the Minister. This establishes a dilemma for ensuring transparency and autonomy in internal checks regarding acts of the Minister and NITA-U.

Section 19(3) of the NITA-U Act provides that:

---

52 See Section 5(3) of the NITA-U Act.
53 See Section 5(e) of the NITA-U Act.
54 See Section 5(6) of the NITA-U Act.
55 See Section 19(1) of the NITA-U Act.

while conducting the survey, data collection by the designated officers involves use of search warrants and summons.

The authorised officer involved in data collection may extend the scope of information prescribed in a warrant to involve any data he considers pertinent to the survey being conducted.[56] The requested person must give all required information or access to a device to the authorised officer in the time prescribed in the search warrant.[57]

Section 21 of the NITA-U Act grants NITA-U officials authority, during "reasonable times", to enter upon, inspect and make inquiries thought to be relevant to a technology survey being conducted. The Act is silent on the meaning of "reasonable times". The Act criminalises obstruction of Authority officials in the discharge of their lawful obligations.[58] It is also an offence to withhold any information or device required by the Authority officials in the conduct of the survey.[59] The prescribed punishment upon conviction is a six-month jail term or a fine not exceeding 12 currency points or both.[60]

However, the statute is silent on the goals and objectives of conducting the information technology surveys. The broad undefined search, inquiry and seizure powers granted to the state officials with respect to conducting the cyber-related surveys generate unpredictability and ambiguity in the enforcement of the law, with foreseeable violations of the internet freedoms of the citizens. This is aggravated by a lack of clarity about the nature and scope of the information required by NITA-U. The system is devoid of autonomous checks and thus falls short of international standards for enhancing a transparent and predictable system. The statute also creates an opportunity for unlawful surveillance and abuse of the right to privacy by enabling the installation of spyware and unlawful access to personal data by third parties.

Further, sections 34-39 of the NITA-U Act grant wide and unchallenged powers to the Minister of Information and Computer Technology to make directives and make regulations necessary for implementing the Act, including declaring acts that amount to crimes under the

56 See Section 20(1) of the NITA-U Act.
57 See Section 20(2) of the NITA-U Act.
58 See Section 38 of the NITA-U Act.
59 See Section 38(4) of the NITA-U Act.
60 See Section 38(5) of the NITA-U Act.

Act and prescribing punishment for such offences. The checks and balances established under the statute are weak and create an enabling environment for abuse of power by the Minister.

3.13 Regulation of Interception of Communications Act

This statute came into force on 3 September 2010. The Regulation of Interception of Communications Act (RICA) obligates the Minister of Security to establish and maintain a communication interception Monitoring Centre.[61] The Act also provides that lawful interception may be authorised by the Minister upon application by authorised persons. Section 4 of RICA provides that said authorised persons are the heads of the various security agencies, namely, Uganda People's Defence force, Uganda Police, External Security Organisation and Internal Security Organisation. RICA also requires the Chief Justice to designate a judge for the purpose of granting warrants of interception under the Act.[62] Whereas the Act lists grounds upon which a warrant of interception may be issued, the law paves the way for the issue of a warrant upon proof of a legitimate interest, as opposed to proof of existence of substantial reasonable grounds.[63] The evidentiary burden to be discharged by officials is weak.

This creates an opportunity for abuse of functions by the officials for personal interests and political persecutions. The system also lacks impartial, independent and competent checks and balances. This is evident in the Chief Justice having sole power in designating judges for the implementation of RICA.[64] RICA bases the grounds for application of a warrant of interception on threats to the national economic interest.[65] However, the statute is silent on the meaning of national economic interest. This imprecision and ambiguity in defining key concepts in the enforcement of RICA create an environment for loose interpretation, potentially to the detriment of innocent citizens.

61 See Section 3 of RICA.
62 See Section 1(b) of RICA.
63 See Sections 5, 6 & 7 of RICA.
64 See Section 1 of RICA.
65 See Section 5 of RICA.

Section 9 of RICA obligates telecommunication companies to ensure registration of all SIM cards issued to users. The process of registration involves the creation and maintenance of a database of all registered customers of the telecommunication firms. The Act does not provide details relating to maintaining the data bases by these firms. It bears noting that majority of the telecommunication firms are multinational corporations with their administrative systems in foreign states. This creates opportunities for illegal access to personal data of Ugandans by third parties, especially in the countries where these companies are headquartered. Contrary to international standards calling for consent of the person whose information is sought, the telecommunication companies can give personal data to other public and private agencies upon request, without seeking the affected person's consent. This is a gross violation of the established regional and international standards relating to the nature and justification of limitations upon enjoyment of internet freedom.

Section 10 of RICA provides for access to and disclosure of protected data. Section 1 of the Act defines protected data as data encrypted by a key. The protected information can be obtained by serving notice on a person believed to be in possession of the information. The Act permits authorised officers to act as intermediaries in obtaining the protected information. However, the authorised official may issue a notice of disclosure of protected information on a person upon belief that:

> a key to any protected information is in the possession of any person; the imposition of disclosure requirement in respect of the protected information is necessary; it is in the interest of national security; the same is for the purpose of preventing or detecting an offence of drug trafficking or human trafficking; and it is in the interest of the economic well-being of Uganda.[66]

The notice of disclosure has to be in writing, detailing the time limits for compliance and the information required.[67]

RICA presents a lot of undefined, imprecise and unclear terminology, procedures and terms of reference for the officials involved in its implementation. Further, RICA contains gaps that curtail efficiency in its implementation. The low evidential threshold which allows for the

66 See Section 10(1) of RICA.
67 See Section 10(2) of RICA.

issuing interception warrants on proof of "reasonable" grounds by the authorised officers creates an environment for abuse of process and violation of the right to privacy.[68] Amnesty International calls for explicit provisions requiring judicial authorisation for disclosure of protected information.[69]

3.14 Electronic Signatures Act

The Electronic Signatures Act (ESA) was enacted to regulate use of electronic signatures in e-transactions. Section 2 of the Act presents a gap in the regulation of data flow and use of electronic signatures in Uganda. The definition of "electronic signature" provided by the Act is ambiguous. These gaps in the law pose a threat of cyber-attacks by aiding identity discovery of persons using an electronic signature.

Part IV of the Act mandates NITA-U to manage, monitor and control key public infrastructure.[70] Section 88 gives a police officer unfettered and broad powers to:

> access any computerised data whether stored in a computer or otherwise. For purposes of this section "access" includes being provided with the necessary password, encryption code, decryption code, software, or hardware and any other means required to enable comprehension of computerised data.[71]

The ambiguity in processes and measures used by NITA-U in granting licences to service providers, maintenance of the established data base, and arbitrary investigative powers pose a risk of violation of the fundamental human rights of citizens.[72]

3.15 Computer Misuse Act

The Computer Misuse Act (CMA) penalises unauthorised access to computer programmes and data, unauthorised modification of computer material, and unauthorised use of interception of computer programmes.[73] The law prescribes jail terms of 10-15 years for the various offences contained in the Act.[74] The gravity of these sanctions has an unnerving effect on the enjoyment

68 Amnesty International (2010) at 29.
69 Amnesty International (2010) at 30 & 31.
70 See Section 22 of the ESA.
71 See Section 88 of the ESA.
72 UN Special Rapporteur (2013) para 47.
73 See Section 5 of the CMA.
74 See Sections 5, 7, 15, 19, 21, 24, 25 & 26 of the CMA.

of internet freedoms. Section 18 of the CMA penalises unauthorised disclosure of information thus:

> any person who accesses any electronic data, record, book, register, correspondence, information, document or any other material is bound to keep the said information secret and protected from third parties.

This provision curtails enjoyment of freedom of expression and opinion. It hinders free dissemination of information and imparting of opinions, as required under regional and international law.

Section 9 of the CMA provides that:

> an investigative officer may apply to court for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.

The officer only has to prove the existence of reasonable grounds of likely loss or modification of the data in question. The evidential burden on the investigative officer is far below the required standards. The expeditious preservation order remains in force until the investigations into the offence are concluded or, where prosecution is instituted, until the final determination of the case, or until such time as the court deems fit or directs.[75]

The CMA is silent on the standard of proof required in an application for an expeditious preservation order. The "reasonable" ground test is an insufficient test to be applied across all crimes listed in the Act. It poses a great risk of a preservation order being issued on the basis of mere suspicions, which risks violation of the right to privacy. The law does not provide a remedy to a victim of ill-considered preservation orders. Thus, the injustice likely to be suffered by the victim will go uncured. This breeds an imprudent culture of using state agencies for promoting private or third-party interests at the expense of fundamental human rights.

Section 10 of the CMA authorises investigative officers to apply to a competent court for a disclosure order in respect of preserved data. The order so obtained applies to all service providers and modes involved in the transmission of the data. Section 11 of the CMA allows that where the investigation or prosecution of a crime under the Act necessitates obtaining

75 See Section 9(3) of the CMA.

information in a person's control, the investigating officer may apply for a court order compelling said person to disclose the information within his knowledge. The court is bound by the requests listed in the application for the order. This system negates judicial impartiality and independence as it amounts to an attack upon judicial discretion in the trial procedure. Further, the provision creates an opportunity for the abuse of court process by the investigative officers.

Section 28(2) of the CMA provides that:

> an authorised officer may seize any computer system or take any samples or copies of applications of data that is concerned in or is on reasonable grounds believed to be concerned in the commission of an offence, whether within Uganda or elsewhere.

It bears noting that the Act does not explain what amounts to "reasonable grounds" with regard to the above provision. The information sought often may not be proportional to the crime being investigated or prosecuted. The provisos under the CMA are shy of personal privacy guarantees as software and devices used are interconnected with the service provider's cyber network over which the victim lacks access and control. These provisions have had far-reaching effects on the enjoyment of cyber space. This is because state agencies and private institutions control and manage personal data in disregard of the fundamental rights and interests of the people.

In addition, the CMA gives broad and unclear powers to police officers regarding search and seizure of data or devices, based on suspicion of a potential perpetrator's plan to commit a computer-related offence under the Act. Section 28 of the CMA confers jurisdiction upon Magistrates' Courts, upon demonstration of reasonable grounds by a police officer that crime is about to be committed in any premises, to grant a search and seizure warrant. The police officer may use reasonable force in execution of the search warrant. Section 28(9) of the CMA describes premises which may be searched as: "Any land, building, movable structure, vehicle, vessel, air craft and hover craft."

Seizure extends to materials such as computer hardware, software and copies of computer-generated data which, on reasonable assessment, are believed to be or actually are connected to the investigation or prosecution of a given offence.[76] The evidential burden is

76 See Section 28(2) of the CMA.

weak as it hinges on proof of existence of reasonable grounds. The Act is silent on what amounts to "reasonable grounds". This trend creates a risk of abuse of fundamental human rights since the Act leaves the determination of "reasonableness" to the personal assessment of criminal justice officers.

Therefore, it may be concluded rightly that unchallenged, undefined and ambiguous authority conferred upon security operatives suggests a likely use of a subjective test for the granting of court orders under the Act, which poses a risk of curtailing enjoyment of internet freedoms. The ability to access personal data, especially by security agencies, largely is unchallenged.[77]

3.16 Electronic Transactions Act

This Act regulates the use, security, facilitation and regulation of electronic communications and transactions. The Act exonerates service providers from civil or criminal liability regarding third-party data in the form of electronic records to which they merely provide access.[78] However, for one to rely on this "immunity", the liability should be founded upon the making, publication, dissemination or distribution of material or a statement in such material or the infringement of any rights subsisting in or in relation to the material in question.[79] This protection is limited to non-contractual obligations.[80] Therefore, a network service provider is criminally liable with regard to obligations arising from a licensing or regulatory framework established by law or an obligation imposed by law or a court to remove, block or deny access to any material or data.

The Electronic Transactions Act relieves service providers of liability in specific circumstances. Section 30 provides that:

> where a service provider refers or links users to a data message containing an infringing data message or infringing activity, the service provider is not liable for damage incurred by the user if the service provider does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of the user; service provider is not aware of the facts or circumstances from

77 UN Special Rapporteur (2013) paras 48 & 49.
78 See Section 29 of the Electronic Transactions Act.
79 See Section 29(1)(a) & (b) of the Electronic Transactions Act.
80 See Section 29(2)(a) of the Electronic Transactions Act.

> which the infringing activity or the infringing nature of the data message is apparent; service provider does not receive a financial benefit directly attributable to the infringing activity; and removes or disables access to the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to the data message infringes the rights of the user.

Section 31 of the Act provides that notification of infringement to the service provider must be in writing. Whereas the Act provides for efforts by service providers to withdraw an unlawful data message, it is silent about reference to courts of law for an order to have the data deleted from the system. The Act also does not spell out procedures to be undertaken by the service provider prior to withdrawal of an unlawful data message. The meaning of the concept of "unlawful data" for purposes of Section 31 is not explained in the statute. This creates an avenue for violation of the right to privacy, especially by third parties who may exploit this gap in the law.

Section 32 of the Act suggests that monitoring data transmitted or stored or making inquiries regarding an unlawful activity are discretionary for the service providers. The Act obligates the Minister, in liaison with NITA-U, to establish and supervise procedures for reporting unlawful transactions or dissemination of illegal information to competent state agencies.[81] However, there is no statutory instrument or policy guide relating to disclosure of illegal activities to public authorities by service providers.

This widens the existing enforcement gap, as such provisions create a dilemma among law enforcement officers. The Electronic Transactions Act does not provide remedies for potential victims of unlawful interference with their internet freedom in the process of transmission of data between the service providers and the public authorities. This contravenes the accepted regional and international standards which require states parties to promote and respect fundamental human rights, particularly the right to privacy and the freedoms of expression and opinion.

81 See Section 36 of the Electronic Transactions Act.

3.17 Uganda Communications Act

The Uganda Communications Act (UCA) of 2013 regulates the communications system in Uganda. Section 4 of the UCA establishes the Uganda Communications Commission (UCC). The Commission is obligated to:

> Implement the objectives of the Act; monitor, inspect, review, licence, supervise, control and regulate communications services; to conduct or authorise any person to conduct technical evaluations relating to communications services; to coordinate and collaborate with the relevant national and international organisations in matters relating to communications; to set national standards and ensure compliance with national and international communications services and equipment; to improve communications services generally and to ensure equitable distribution of services throughout the country; to promote competition, including the protection of operators from acts and practices of other operators that are damaging to competition, and to facilitate the entry into market of new and modern systems and services; to advise government on communications policies and legislative measures in respect of providing and operating communications services; to regulate interconnection and access systems between operators and users of telecommunications services; to set standards, monitor and enforce compliance relating to content; to represent Uganda's communications sector at national and international fora and organisations relating to its functions and to coordinate the participation of any interested groups; and carry out any other functions that is related to the functions of the commission.[82]

Section 8 of the UCA provides for the independence of the Commission in the discharge of its lawful duties. However, the Minister may issue policies, guidelines and codes for the UCC necessary for performance of its mandate.[83] The UCA bestows broad and unfettered authority on the Commission in the performance of its obligations. These unchallengeable powers can be abused and have been abused to the detriment of the enjoyment of internet freedoms as, for example, in the establishment and maintenance of social media and communication interception monitoring centres in exercise of the authority conferred upon the Commission by RICA and the UCA.

These centres have been used to promote the political interests of the current political regime by allowing information gathering for political persecution. The reports generated by these centres also resulted in the state imposing a social media tax, which is a prerequisite for a person to access social media and search engines such as Google. The statute contains no procedures and mechanisms for the handling of the personal data to which the officers at these

82 See Section 5 of the UCA.
83 See Section 7 of the UCA.

centres have access. This creates susceptibility to unlawful access of personal data by a third party. It amounts to a gross violation of the right to privacy and freedom of expression protected by international statutes, such as the ICCPR, which Uganda has signed or ratified.

3.18 Anti-Pornography Act

The Anti-Pornography Act (APA) criminalises all acts related to pornography. It was enacted in 2014. Section 13 of the Act provides that:

> a person shall not produce, traffic in, publish, broadcast, procure, import, export, sell or abet any form of pornography.

A crime under the APA attracts a maximum jail sentence of 10 years or a fine not exceeding 500 currency points.[84] Child pornography is criminalised in Section 14 and attracts a jail sentence of 15 years or a fine not exceeding 50 currency points. The Pornography Control Committee is charged with the duty of implementing the Act. Pornography is defined as:

> any representation through publication, exhibition, cinematography, indecent show, information technology or by whatever means, of a person engaged in real or stimulated explicit sexual activities or the representation of the sexual parts of a person for primarily sexual excitement.[85]

The APA adopts an extreme approach to combating pornography. This means that all modes of pornography are prohibited, including both practical operations and the use of media. According to the Unwanted Witness Report of 2014, the approach adopted by the APA in defining "pornography" is imprecise. It hinders media houses and individuals from knowing what actually amounts to pornography.[86] The UN Special Rapporteur on the Right to Privacy and Freedom of Expression posits that states are required only to criminalise child pornography;[87] arbitrary use of criminal sanctions to curtail enjoyment of internet freedoms is unjustified.

The APA suggests heavy punishments for all pornography offences. The Act attempts to criminalise all forms of pornography, which violates freedom of expression as it hinders an

84 See Section 13(2) of the APA.
85 See Section 2 of the APA.
86 UN Special Rapporteur (2012) paras 34 & 35.
87 UN Special Rapporteur (2012) para 32.

individual's opportunity to seek or share information that may be viewed as pornographic. The determination of the scope of pornographic substance lies with the authorities, and it is not clearly described in the statute. Whereas the anti-pornography campaign has moral support, the fundamental human rights of other people should be tolerated. There is a need for tolerance in a society built on unity in diversity.

Section 3 of the Act provides for the establishment of the Pornography Control Committee. Section 24 requires the Committee to establish and maintain a database of those prosecuted for or convicted of offences under the Act. The details to be captured in the system include the name of the person, the punishment, the offence and the date of conviction. This is an infringement of the right to privacy of an individual. Pornography is categorised as one's private affairs and thus should not be the target of unlawful interception or interference. Commentators on section 24 of the APA point to the need for using the "shame them" theory to deter criminality.[88]

Section 15 of the APA vests jurisdiction in the courts to grant arrest, search and seizure warrants against a person suspected of being in possession of pornographic material or performing an act or an event with a pornographic connotation. The section provides that:

> where information is brought to the of the court that there exists in premises, an object or material containing pornography or an act or event of a pornographic nature, the court shall issue a warrant for the seizure of the object or material and for the arrest of the person promoting the material or object. An authorised person in possession of a search warrant issued by the court may enter any premises and inspect any object or material or gadget for the purpose of giving effect to this Act. A person who obstructs an authorised person in the carrying out of any of the function under this section commits an offence and is liable, on conviction, to a fine not exceeding two hundred and fifty currency points or imprisonment not exceeding 5 years or both.

Authorised officers are likely to exploit this deficit to access a person's devices or data for private or third-party benefit.[89] The gap may be utilised also to instal communication surveillance software or gadgets in the seized devices. The Act provides unclear procedures and mechanisms for handling the seized devices or materials. This creates an opportunity for

88 UN Special Rapporteur (2012) paras 33 & 34.
89 UN Special Rapporteur (2011) para 81.

alteration or modification of an individual's cyber system or network to his or her detriment. It amounts to suppression of the right to privacy and freedom of expression.

The APA imposes criminal liability upon internet service providers who, by failing to use or enforce measures established by the Pornography Control Committee, authorise uploading or downloading any pornographic material through their service or links. The APA stipulates a jail sentence of five years or a fine not exceeding 250 currency points for one convicted of an offence under section 17. With respect to firms, the court may direct termination of their business.[90]

3.19 Conclusion

This chapter has discussed the various regional and international standards regarding protection of the right to privacy and freedom of expression and opinion. States parties are urged to guarantee internet freedoms. However, enjoyment of internet freedoms is not absolute. Limitations upon these rights should be activated only upon fulfilment of the three-fold test contained in Article 19(3) of the ICCPR and other related regional and international instruments, such as the ACHR, ECFR and ACHPR.

The chapter also presented a critique of the cyber law of Uganda in relation to the established regional and international standards. This law largely falls short of these standards with respect to the enjoyment of internet freedoms. The discussion has identified gaps in the cyber law regime of Uganda. These gaps pertain to ambiguous provisions, undefined key concepts, such as the "national interest", and unfettered powers conferred on security agencies and other law enforcement units, which encourage human rights violations.

90 See Section 17(2) of the APA.

CHAPTER FOUR

CONCLUSION AND RECOMMENDATIONS

4.1 Conclusion

This research paper has criticised the cyber-related law of Uganda against the regional and international standards regarding the right to privacy and freedom of expression. Uganda has ratified instruments containing these standards, such as the International Covenant on Civil and Political Rights. The Constitution of the Republic of Uganda guarantees the right to privacy and freedom of opinion, expression and assembly.[1] However, the study reveals a trend of violation of these rights by private and public institutions. A greater percentage of these violations are by state security agencies, such as the Uganda Police, Internal Security Organisation and Communications Surveillance Monitoring Centre under the guise of protecting an undefined national interest.

The cyber security phenomenon is of global concern and crucial in the enjoyment of computer-related freedoms. The research asserts that technological development is a dynamic aspect that needs to be protected at all times. This involves protection from illegal or unlawful interference with an individual's reputation, integrity, family, correspondence and confidentiality. The research established that the existing computer-related laws of Uganda are contradictory.

There is a global consesus that states parties should guarantee the enjoyment of the right to privacy and of freedom of expression. This may be inferred from the various regional and international instruments, commentaries, reports and research papers by distinguished academicians, writers and UN Special Rapporteurs on the right to privacy and freedom of expression. It is worth noting that the right to privacy and freedom of expression are interwoven with other fundamental human rights, such as the rights to life, education and

1 See Articles 26 & 27 of the 1995 Constitution of Uganda.

health. The right to privacy and freedom of expression are therefore crucial for human development and should be protected at all times. It is agreed widely also that these rights are not absolute and can be subject to limitations. International law suggests that restrictions upon enjoyment of the right to privacy and freedom of opinion should be:

- clearly defined and prescribed under the law of the state party;
- necessary for protection of state security, public order, public health, morals, and other people's rights and freedoms; and
- able to satisfy the principle of proportionality.[2]

The research has highlighted gaps in the regional, international and Ugandan cyber-related framework regarding the enjoyment of cyber freedom. Worse still, computer-related laws in Uganda fall short of the established regional and international standards for the protection and regulation of the right to "internet freedom". This problem is aggravated by a widespread ignorance of internet freedoms among the Ugandan population.[3] People generally are unaware of cyber-related law, avenues through which to pursue their rights when violated, and the procedure to be followed to maximise enjoyment of their internet freedoms. The *lacunae* disclosed by this research include the following:

- ambigous provisions relating to the regulation of cyber space and cyber sytems in Uganda;
- application of the "reasonable ground" test in a rather subjective manner, which creates room for violation of fundamental rights and abuse of functions by state officials;
- key concepts — such as "national security" — in computer-related law are undefined, leading to their frequent misuse to justify restrictions upon internet freedoms;
- lack of credible, transparent checks and balance mechanisms in the law governing Uganda's enforcement agencies;
- the absence from the existing legal framework of remedies for victims of violations of the right to privacy and freedom of expression;

2 UN Special Rapporteur (2013) paras 24, 25 & 27.
3 Mayambala (2016) at 9.

- the hortatory nature of the majority of the provisions in regional and international instruments related to safeguarding of the right to privacy and freedom of opinion;
- certain of the computer-related laws in Uganda require establishment and maintenance of databases of personal details of Ugandans by various agencies, such as telecommunications companies and monitoring centres;
- statutes such as the Regulation of Interception of Communications Act, the Uganda Communications Act and the Anti-Terrorism Act confer unfettered authority upon officials, which authority often has been used to curtail enjoyment of internet freedom (as, for example, in the social media shutdown during the 2016 Presidential Elections);[4] and
- the Anti-Pornography Act, in taking an extreme approach and criminalising all acts of pornography, curtails enjoyment of freedom of expression and opinion.

4.2 Recommendations

4.2.1 Amendment of Laws

This recommendation is premised on the need to bridge the gaps disclosed by this study. The amendments are necessary at national, regional and international level in order to create an environment for the full enjoyment of cyber freedoms. The regional and international instruments ought to be amended to include mostly mandatory provisions regarding the guarantee, observation and regulation of the right to privacy and the freedoms of opinion, expression and information.

Other key areas to be addressed by amendments include: constitutional guarantees for victims of unlawful cyber attacks or communication intereptions; internal checks for monitoring and surveillance agencies; clear definitions and scope of fundamental rights; transparent procedures in obtaining and handling of personal data by private and public institutions; prevention of the use of anonymous identification tags on internet-related media; and the

4 Maverick (2016) at 14.

adoption of an objective test in the granting of court orders pertaining to implementation of cyber-related law.

4.2.2 Creation, Maintenance and Facilitation of Specialised Units at Regional and International Level

Specialised units should be created by the regional and international institutions — such as the AU, ECOWAS, SADC, the EU, and the UN — mandated to monitor implementation of regional and international instruments by the states parties. This is premised on the role played by these institutions in standard setting regarding the protection of fundamental human rights. Non-compliant states ought to be sanctioned. These sanctions may take the form of travel bans upon officials indicted for or convicted of violation of fundamental human rights. The efforts of the specialised units will aid the transformation from "paper" law to practice.

At the national level, Uganda should establsih and maintain insitutions which safegaurd internet freedom. These institutions should be made accessible to the victims of cyber attacks or infringement of internent freedoms. All countries should embrace international co-operation to cater for the dynamics in the information technology sector.

4.2.3 Research and Awareness Creation

This can be done through organising or facilitating cyber-related training, seminars, conferences, innovations and research projects. Awareness creation should be conducted for all participants in the information and technology sector. This willl help to lessen the existing knowledge gap in the use of the cyber space. Further, enforcement deficit will be reduced, since there will be harmonious implementation of the law. Also, innovation encourages domestic creation of software which protects citizens from unlawful and unnecessary communication interception by foreign countries or their agencies (such as the CIA).

The government should offer and facilitate specialised cyber training for security officers. The rationale is to cater for the gaps in detecting, investigating and prosecuting cybercrimes in Uganda. Recent trends indicate that cyber-related crimes are becoming rampant. In addition, the lapse in the criminal justice system has facilitated the commission of

conventional crimes such as murder, rape and terrorism with the aid of cyber tools. The growing reliance of courts upon electronic evidence in criminal cases justifies equipping security officers with cyber knowledge.

4.2.4 Cyber Filtering

The government should implement internet filtering services to prevent access to morally or socially harmful websites, especially those connected to pornography and terrorist agendas. The specialised units could do continous internet filtering also. However, the process of filtering should be tansparent, so as to prevent abuse of power by those mandated to conduct the cyber filtering. This is a preventive strategy against cyber attacks and the dissemination of harmful messages, propaganda and ideologies. It will prevent unnecessary and illegal interference with the personal data of Ugandans under cover of protecting state security, the national interest and the morals and values of the citizenry.

4.2.5 Enhance Regulation of Cyber-Related Service Providers

There is a need to regulate and monitor all categories of internet service providers, in both the public and private sectors. The purpose is to prevent them from being used as crime commission havens. It would involve enacting laws, implementing policies and establishing monitoring institutions to control access to prohibited internet sites and service providers. An example would be a law prohibiting children access to internet cafes, strip clubs and pornography shops. The use of unique identities which are traceable should be encouraged in order to enhance the investigation of cybercrime and the prosecution of perpetrators.

BIBLIOGRAPHY

PRIMARY SOURCES

International Legal Instruments

African Charter on Human and Peoples' Rights, adopted on 1 June 1981 and came into force on 21 October 1986.

African Declaration on Internet Rights and Freedom, adopted on 4 November 2016.

African Platform for Access to Information Declaration, adopted on 19 September 2011.

African Union Convention on Cyber Security and Personal Data Protection, adopted on June 27 2014 and came into force on March 14 2018.

European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols 11 and 14, adopted on 4 November 1950 and came into force on 3 September 1953.

European Union Charter on Fundamental Rights, adopted on 7 December 2000 and came into force 1 December 2009.

International Covenant on Civil and Political Rights, adopted on 16 December 1966 and came into force on 23 March 1976.

Joint Declaration on Freedom of Expression and the Internet, adopted on 1 June 2011.

Universal Declaration of Human Rights, adopted on 10 December 1948.

Ugandan Legislation

Anti-Pornography Act of 2014.

Anti-Terrorism Act of 2002.

Computer Misuse Act of 2011.

Constitution of the Republic of Uganda of 1995.

Electronic Signatures Act of 2011.

Electronic Transactions Act of 2011.

Evidence Act Chapter 6 of 2000.

National Information Technology Authority Act of 2009.

Regulation of Interception of Communications Act of 2009.

Uganda Communications Act of 2013.

Case Law

Amama Mbabazi v Museveni & Ors [2016] UGSC.

Attorney General v Salvatore Abuki Constitutional Appeal No 1 of 1998.

Attorney General's Reference No 1 of 1991.

Cox v Riley [1986] 83 Criminal Appeal.

Dubská and Krejzová v Czech Republic Applications 28859/11 and 28473/12.

R v Bow Street Magistrate; ex parte US Government Allison [1998] Cr.App.R.

R v Gilham [2009] EWCA.

Uganda v Dr Aggrey Kiyingi [2006] UGHC.

Uganda v Garuhanga and Mugerwa CR 17 of 2004 Buganda Road Court.

Uganda vs Kato Kajubi [2010] UGCA.

SECONDARY SOURCES

Books

Alkaabi A, Mohay G, McCullagh A & Chantler N (2011) *Dealing with the Problem of Cybercrime* Springer Berlin: Heidelberg.

Bainbridge D (2007) *Introduction to Computer Law* Pearson Education Limited: Edinburgh.

Casey E (2004) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* Elsevier Academic Press: London.

Chawki M, Darwish A, Khan AM & Tyagi S (2015) *Cybercrime, Digital Forensics and Jurisdiction* Springer: New York.

Jakobsson M & Myers S (eds) (2006) *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* John Willy & Sons Inc. Hoboken: Canada.

Kizza JM (2007) *Ethical and Social Issues in the Information Age* Springer: New York.

Sofaer AD & Seymour EG (eds) (2001) *The Transitional Dimension of Cybercrime and Terrorism* Hoover Institution Press: United States of America.

Stevens T (2016) *Cyber Security and the Politics of Time* Cambridge University Press: London.

Journal Articles

Bainbridge D (2007) "Criminal Law Tackles Computer Fraud and Misuse" 23(3) *Computer Law & Security Journal* 276-281.

Beagle NA (2011) "Modern Stalking Laws: A Survey Of State Anti-Stalking Statutes Considering Modern Mediums And Constitutional Challenges" 14 *Chapman Law Review* 467-468.

Cassim F (2009) "Formulating Specialised Legislation to Address the Growing Spectre of Cybercrime: A Comparative Study" 12(4) *Potchefstroom Electronic Law Journal* 36-79.

Coetzee SA (2013) “Learner Sexual Offenders: Cyber Child Pornography” 4(11) *Mediterranean Journal of Social Sciences* 752-757.

Barry C (1997a) “The Future of Cyber Terrorism, Crime and Justice International” 13(2) *Crime and Justice International Journal* 15-18.

Barry C (1997b) “The Future of Cyber Terrorism” 13(2*) International Crime and Justice International Journal* 35-41.

Embar-Seddon A (2002) “Cyberterrorism: Are We under Siege?” 45(6) *American Behavioural Scientist* 1033-1044.

Glyn EA (1983) “Computer Abuse: The Emerging Crime and the Need for Legislation” 12(1) *Fordham Urban Law Journal* 73-101.

Hansen-Young T (2005) “Whose Name Is It, Anyway? Protecting Tribal Names from Cyber Squatters” 10(6) *Virginia Journal of Law and Technology* 1-18.

Iqbal M (2004) “Defining Cyber Terrorism” 22(2) *The John Marshall Journal of Information Technology and Privacy Law* 397-408.

Jeffery RC (1957) ‘’The Development of Crime in Early English Society’’ 47(6) *The Journal of Criminal Law, Criminology and Police Science* 647-666.

Joyner CC & Lotrionte C (2002) “Information Warfare as International Coercion: Elements of a Legal Framework” 12(5) *European Journal of International Law* 825-865.

Kilian M (2000) “Cybersquatting and Trademark Infringement” 7(3) *Murdoch University Electronic Law Journal* 23-46.

Kokott J & Sobotta C (2013) “The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECTHR” 3(4) *International Data Privacy Law* 222-228.

Mishler JL (2000) “Cyber Stalking: Can Communication via the Internet Constitute a Credible Threat and Should an Internet Service Provider Be Liable if it Does” 17(1) *Santa Clara Computer & High Technology Law Journal* 115-138.

Pollicino O (2010) “The New Relationship between National and the European Courts after the Enlargement of Europe: Towards a Unitary Theory of Jurisprudential Supranational Law?” 29(1) *Yearbook of European Law* 65-111.

Power R (2002) “CSI/FBI Computer Crime and Security Survey" 17(2) *Computer Security Journal* 2-29.

Treadwell L (2013) “50 Ways to Protect Your Identity in a Digital Age: New Financial Threats You Need to Know and How to Avoid Them” 5(2) *Journal of Multi-Disciplinary Research* 105-108.

Tumushabe T & Baryamureba V (2007) “Cyber Crime in Uganda: A Myth or Reality?” 1(8) *International Journal of Computer and System* 377-381.

Visser J, Oosthuizen H & Verschoor T (2014) “A Critical Investigation into Prosecutorial Discretion and Responsibility in the Presentation of Expert Evidence” 131 *South African Law Journal* 865-882.

Wold G (2007) “Computer Crime: The Undetected Disaster” 31 *Disaster Recovery Journal* 124-127.

Theses

Chibuko RO "The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions" (Unpublished Doctor of Philosophy thesis, University of Stirling, 2015).

Nambasa S "Formation of a Company: What Uganda Could Learn from South Africa's Modified System" (unpublished LLM thesis, University of Cape Town, 2014).

Online Publications

Amnesty International (2011) "Restrictions on the Rights of Freedom of Expression and Peaceful Assembly in Uganda", available at *https://www.amnesty.org/en/documents/AFR59/016/2011/en/.37* (visited 13 March 2018).

Berry C "The Act of Cybercrime", available at *https://www.masthead.co.za/newsletter/the-act-of-cybercrime/* (visited 29 May 2018).

Biegel S (2001) "Beyond our Control? The Limits of our Legal System in the Age of Cyberspace", available at *http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech539.pdf* (visited 3 June 2018).

Commission of the European Communities (2007) "Towards a General Policy on the Fight against Cybercrime", available at *https://pure.uva.nl/ws/files/1542922/152721_406308.pdf* (visited 31 May 2018).

Lynch J (2014) "Identity Theft in Cyberspace: Crime Control Methods and their Effectiveness in Combating Phishing Attacks", available at *http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1517&context=btlj* (visited 4 June 2018).

Mayambala KR (2016) "Examining the Nexus between ICT and Human Rights in Uganda: A Survey of the Key Issues", available at *https://idlbncidrc.dspacedirect.org/bitstream/handle/10625/41475/129275.pdf* (visited 25 August 2018).

Ministry of Information and Communications Technology (2011) "National Information Security Strategy", available at *http://www.ict.go.ug/sites/default/files/Resource/ICT_Policy_2014.pdf* (visited 14 March 2018).

Mwaita P & Owor M (2013) "Workshop Report on Effective Cybercrime Legislation in Eastern Africa", Dar es Salaam Tanzania, available at *https://rm.coe.int/16802f2349* (visited 13 March 2018).

Uganda Communications Commission (2017) "Report on Status of Internet Users March 2017", available at *http://www.internetworldstats.com/af/ug.htm* *and* *http://www.ucc.co.ug/rcdf/* (visited 11 March 2018).

Uganda Police (2017) "Annual Crime and Road Safety Report of 2017", available at *https://www.osac.gow/pages/contentReportDetails.aspx?cid=2178* (visited 13 March 2018).

UN Special Rapporteur on Freedom of Expression (2011) "Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression", available at *https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf* (visited 23 July 2018).

UN Special Rapporteur on Freedom of Expression (2012) "Report of the United Nations High Commissioner for Human Rights", available at *http://www.childlinesa.org.za/wp-content/uploads/un-report-of-the-united-nations-high-commissioner-for-human-rights-2012.pdf* (visited 14 March 2018).

UN Special Rapporteur on Freedom of Expression (2013) "Report on the Implications of States Surveillance of Communications on the Exercise of the Human Right to Privacy", available at *http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx* (visited 13 March 2018).

United Nations General Assembly Resolution (2009) "Creation of a Global Culture of Cyber Security and Taking Stock of National Efforts to Protect Critical Information Structure", available at *https://undocs.org/A/RES/64/211* (visited 12 March 2018).

United Nations Human Rights Committee (2011) "General Comment No 34 on Article 19: Freedoms of Opinion and Expression", available at *https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf* (visited 12 June 2018)

United Nations Resolution (2004) "Security Council Resolution on Threats to International Peace and Security Caused by Terrorist Acts"**,** available at *https://www.un.org/ruleoflaw/blog/document/security-council-resolution-1566-2004-on-threats-to-international-peace-and-security-caused-by-terrorist-acts/* (visited 3 June 2018).

United States White House (2003) "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets", available at *http://www.whitehouse.gov/pcipb/physical.html* (visited 2 June 2018).

Wald LM (2009) "Making Electricity Distribution Smarter", available at *http://green.blogs.nytimes.com/2009/04/21/makingelectricity-distribution-smarter/* (visited 2 June 2018).

Wilson C (2003) "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress", available at *http://www.dtic.mil/dtic/tr/fulltext/u2/a444799.pdf* (visited 2 June 2018).

Wilson C (2008) "Cyber Terrorism: Vulnerabilities and Policy Issues for Congress", available at *www.fas.org/sgp/crs/terror/RL32114.pdf* (visited 14 March 2018).

Media Sources

James C (1 March 2016) “Museveni vs The People: Elections in A Time of Social Media” *Daily Maverick.*

The Observer (28 February 2018) “Museveni Statement on Murder of Susan Magara”.

Word Count: 18 689