An Annual Publication of Human Rights Awareness and Promotion Forum

HRAPF
HUMAN RIGHTS AWARENESS AND PROMOTION FORUM

THE HUMAN RIGHTS ADVOCATE

FOURTH ISSUE - NOVEMBER 2017

The Computer Misuse Act, 2011: Yet Another Legal Fetter to the Basic Rights and Freedoms of Marginalised Persons

SOURCE: https://www.shutterstock.com

THE HUMAN RIGHTS ADVOCATE

FOURTH ISSUE - NOVEMBER 2017

The Computer Misuse Act, 2011: Yet Another Legal Fetter to the Basic Rights and Freedoms of Marginalised Persons

An Annual Publication of Human Rights Awareness and Promotion Forum

NOVEMBER 2017

Human Rights Awareness and Promotion Forum (HRAPF)
Plot 390, Professor Apolo Nsibambi Road,
Namirembe, Kampala
P.O. Box 25603, Kampala – Uganda
Tel: +256-414-530683 or +256-312-530683
Email: info@hrapf.org Website: www.hrapf.org

EDITOR'S NOTE

It is my pleasure to present to you the fourth issue of *The Human Rights Advocate*. This magazine is an annual publication of Human Rights Awareness and Promotion Forum (HRAPF) that focuses on how particular laws or bills affect the rights of Ugandans, especially marginalised persons. Each issue is dedicated to one law or bill that is analysed by various writers from different angles.

HRAPF is an independent, not-for-profit, non-partisan and non-governmental organisation, which aims to raise awareness and defend the rights of marginalised groups in Uganda. HRAPF strives to advocate for a legal regime that respects and promotes the rights of marginalised persons. This is done through legal research, legislative advocacy, legal and policy analysis, research and documentation and strategic litigation. HRAPF also provides access to justice to marginalised groups through legal aid services provision and legal empowerment.

This fourth issue of *The Human Rights Advocate* is dedicated to the Computer Misuse Act, 2011. This law came under the spotlight recently when the state used its provisions to charge renowned academic, social media activist and government critic Dr. Stella Nyanzi. Through the online social media platform, Facebook, Dr. Nyanzi had used language with sexual imagery to criticise the government for its failure to live up to its promises to provide girls with sanitary pads. In one particular post, she had reportedly referred to the President as a 'pair of buttocks' - something that attracted the charge of cyber harassment under section 24 of the Act. Her other posts were met with the charge of 'offensive communication' under section 25 of the same Act. On an earlier occasion, section 25 was used to charge Mr. Robert Shaka who was thought to be the person using the account of Tom Voltaire Okwalinga (TVO) on Facebook to critique the president and key government officials. It was also used against Mr. Swaibu Nsamba who posted a photoshopped picture of President Museveni in a coffin to show how he would celebrate the President's death.

However, prior to the Dr. Nyanzi, TVO and Swaibu Nsamba cases, this law was already being implemented, albeit without much public attention, against LGBTI persons. HRAPF had registered two cases where suspected members of the LGBTI community were charged under section 25 of the Computer Misuse Act for sending an SMS and posting photos on Facebook, respectively. In the view of HRAPF's legal team, the communications could not be classified as 'offensive' as understood in the context of the Act. The fact that only members of marginalised communities or government critics are charged under the Act, and this following actions to which the application of the Act is questionable, shows that the Computer Misuse Act is being implemented in a targeted way.

The Computer Misuse Act, according to its long title, was enacted 'to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access,

Editorial Team

Editor
Adrian Jjuuko

Sub-editor
Joaninne Nanyange

Reviewer
Linette Du Toit

abuse or misuse of information systems including computers; to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters.' The Act has penal sanctions on computer misuse and also deals with the use of computer programs, references to programs, data content modification, authorised access, investigative measures and procedures. It thus has good intentions, and if applied appropriately, could adequately deal with cybercrime.

> **"It is thus becoming the weapon of choice by prosecutors for use against marginalised persons, their allies and government critics.**

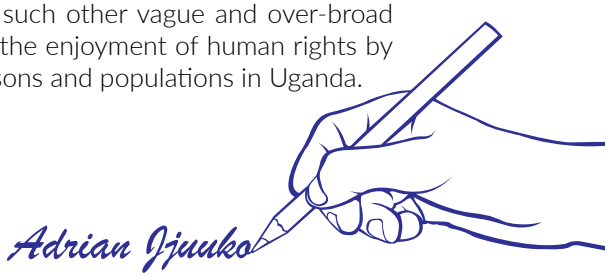
HRAPF's concern with the law is the vagueness of some of its provisions and the targeted prosecutions of unpopular minorities, their allies, and government critics. Section 25 of the Act is particularly problematic. It creates the offense of offensive communications. The provision is vague and thus open to subjective interpretation by the law enforcers. It is thus becoming the weapon of choice by prosecutors for use against marginalised persons, their allies and government critics. It joins a long list of vague provisions that are used to justify the arrest of LGBTI persons and other marginalised persons. Such a provision cannot meet the constitutional requirement that criminal offences be well-defined, and the limited conditions under which the right to freedom of expression may be limited.

It is upon this background that HRAPF has decided to elicit academic reflections and opinions and to publish them in this fourth issue of *The Human Rights Advocate*. The purpose of this issue is to draw the attention of the public to the continuing need to fight the effects of this law, and similar laws, in order to protect and promote the enjoyment of human rights in Uganda.

The magazine contains an editorial, an overview of the Act, a feature, legal and human rights analyses, opinions, and commentaries. The editorial discusses the vague nature of section 25 and calls for a revision of this particular provision. It is followed by the overview of the Act, which discusses the contents and context of the Act. This is followed by a legal analysis of the different provisions based on freedom of expression and the right to privacy. A comparative analysis of similar laws in India, Tanzania and the UK follows. This is followed by an analysis on how the Act fares as regards the international human rights framework. A commentary on the impact of the Act for sexual minorities follows; and then an opinion on how the Act affects Ugandan communicators. This is followed by a commentary on how the Act silences dissenting voices; and finally, a commentary on the rule of law in today's Uganda. Two case updates follow, and the first one is uniquely written by Dr. Stella Nyanzi, the subject of the legal processes; and the second one is on the Robert Shaka case. The Appendix contains HRAPF's statement on the Stella Nyanzi prosecution and the full text of the Act.

As with the previous issues of this magazine, articles have been contributed by a variety of authors representing civil society, academia and the legal profession. The organisation would like to give a special word of thanks to the external authors contributing to this issue: Mr. Edward Ssemambo of Kizza, Tumwesige & Ssemambo Advocates and Board Chair, HRAPF; Ms. Linette du Toit an independent researcher; Dr. Stella Nyanzi of the Makerere Institute for Social Research; Ms. Dorothy Mukasa of Unwanted Witness Uganda; Ms. Arinda Daphine, a story-teller, lawyer and poet and Mr. Andrew Karamagi, a lawyer and political activist. We also thank our staff, Justine Balya, Susan Baluka, Patricia Kimera, Joaninne Nanyange and Adrian Jjuuko for contributing articles.

We hope you find this edition useful, and that the articles herein re-enforce awareness of the need for deliberate advocacy against the use of the over-broad provisions of the Computer Misuse Act as well as such other vague and over-broad laws to curtail the enjoyment of human rights by unpopular persons and populations in Uganda.



Adrian Jjuuko

Editor

Table of Contents

EDITORIAL

Section 25 on Offensive Communications has no place in the Computer Misuse Act

SOURCE: https://www.shutterstock.com

The Computer Misuse Act, 2011 is an important and timely law. There was little that law enforcers could do without an effective legal framework to curb computer cyber crimes. Its long title shows that indeed the law was intended to control the misuse of computers as it provides that it is an Act

> ...to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters.

As is common with the regulation of various social aspects in Uganda, the Act takes the criminalisation approach and imposes heavy punishments for actions that constitute offences under the Act. Most of the criminal offences deal with conduct that is punishable. These include aspects like: unauthorised modification of the contents of computer material (section 14); unauthorised use or interception of electronic communications (section 15); unauthorised obstruction of the use of a computer (section 16); unauthorised disclosure of access codes or passwords (section 17); unauthorised disclosure of information (section 18); electronic fraud (section 19); child pornography through computers (section 23); cyber harassment (section 24); cyber stalking (section 26); provision for preservation orders; searches and seizures (section 28); and provision for the use of electronic evidence in legal proceedings (section 29).

The only provision that if largely out of place is section 25 on offensive communication. This is because whereas all the others focus on using computers to harm others through fraud, extortion, interference with systems, violation of children, among others, this provision focuses on criminalising very broad conduct with the intention of protecting people (read the powerful) from being offended. Vague and ineptly defined provisions violate the right to a fair trial, while protection of people from being offended should not be a legitimate reason for the enactment of a law as that is undue restriction which violates the international standards pertaining to the right to freedom of expression.

HRAPF has in the past, through previous issues of this magazine and various other advocacy tools and avenues, strongly opposed such vague provisions, particularly: Section 44 of the Non-Governmental Organisations Act, 2016 ...

These two aspects both affect the rights of marginalised groups who are the ones most likely to be accused of being offensive to others due to their conduct or behaviour, and at the same time they are also the ones most likely to be targeted by vague provisions that have no clear definition as this helps to have them arrested and 'taught a lesson'. HRAPF has in the past, through previous issues of this magazine and various other advocacy tools and avenues, strongly opposed such vague provisions, particularly: Section 44 of the Non-Governmental Organisations Act, 2016 which imposes undefined obligations upon Non-Governmental Organisations;[1] provisions of the now nullified Anti-Homosexuality Act 2014 on the promotion of homosexuality and aiding and abetting homosexuality;[2] and the now nullified section 15(6)(d) of the Equal Opportunities Commission Act which prevented the Equal Opportunities Commission from investigating matters regarded as immoral or socially unacceptable by the majority.[3] The reason for this opposition is the huge potential and actual impact of such vague provisions on the rights of marginalised groups, particularly LGBTI persons and sex workers.

Section 25 criminalises the wilful and repeated use of 'electronic communication to disturb or attempt to disturb the peace, quiet or right of privacy of any person without purpose of legitimate communication.' Although the head note, describes the offence as 'offensive communication', what is indeed covered in the body of the provision is not offensive communication but rather communication that 'disturbs' someone else's peace, quite or right of privacy. What does it mean to 'disturb the peace, quiet or right of privacy' of another person? Is it sending many messages or publishing what is untrue, or insulting them? What is the test? Do we refer to the subjective intention of the accused to offend or the subjective experience of 'being offended' by the person on the receiving end? Which objective measure should be used? What it actually means is not clear, and so one cannot be sure if what they are doing may be regarded as offensive. This makes actions which can constitute the offence unpredictable and gives law enforcer the discretion to pick and choose what qualifies as offensive. Indeed, any action or communication which has a sexual connotation or concerns sexuality expressed beyond the neatly-drawn boundary lines of majoritarian views can be regarded as 'offensive' and this explains why LGBTI persons and other sexual minorities are most likely to bear the brunt of the law. Indeed, this provision was used against Dr. Stella Nyanzi because her Facebook posts had sexual imagery.

1 This was the subject of the third issue of *The Human Rights Advocate*. The provision still remains on the law books.

2 This was the subject of the second issue of *The Human Rights Advocate*. The Act was declared unconstitutional on procedural grounds by the Constitutional Court of Uganda in the case of *Prof. J Oloka Onyango & 9 Others v Attorney General*, Constitutional Petition No. 009 of 2014.

3 This was the subject of the first issue of *The Human Rights Advocate*. The provision was declared unconstitutional by the Constitutional Court in the case of *Jjuuko Adrian v Attorney General*, Constitutional Petition No. 001 of 2009.

Article 28(12) of the Constitution provides that

Except for contempt of court, no person shall be convicted of a criminal offence unless the offence is defined and the penalty for it prescribed by law.

This implies that in as far as what constitutes this offence is undefined, it is unconstitutional and it should not be applied. This provision therefore violates Article 28(12) of the Constitution, as it violates the fair trial guarantee that a criminal offence should be well defined.

Besides its vagueness, Section 25 also violates the right to freedom of expression as it limits the right beyond constitutionally acceptable limitations. The Constitution, in Article 29(1)(a) guarantees freedom of speech and expression, which includes freedom of the press and other media. The Supreme Court of Uganda, in *Charles Onyango Obbo & Andrew Mujuni Mwenda v Attorney General*[4] made it clear that expression which offends, shocks or disturbs is also protected. The Court also made it clear that whereas the right can be limited, this can only be so under particular circumstances, which meet the limitation test laid down in Article 43. Article 43(1) provides that 'no person shall prejudice the fundamental or other human rights and freedoms of others or the public interest.' Article 43(2)(c) provides that the public interest shall not permit, among others: political persecution, and 'any limitation of the enjoyment of the rights and freedoms prescribed by Chapter Four of the Constitution beyond what is acceptable and demonstrably justifiable in a free and democratic society.' The Supreme Court found that this provision constituted a 'limitation within a limitation' and that it was the right rather than the limitation that had to be given prominence. From this analysis of freedom of expression, it is quite clear that communications that are offensive are still protected under the right to freedom of expression. Section 25 is therefore a violation of this right, as it is a very wide limitation that covers very wide grounds, and is not properly justified. Being offensive is subjective and such a subjective ground should not be the basis for limiting a fundamental right.

The need to balance the protection of individuals from offensive communications with the freedom of expression is important. Whereas individuals should not be allowed to say all they want without any restrictions, the restrictions must be well understood and must serve a purpose that is in the public interest, and which is justifiable in a free and democratic society. To create this balance, other countries do not criminalise offensive communications at all, and those that do, for example the United Kingdom, only criminalise grossly offensive communications and make it clear that the intention must be to cause annoyance, inconvenience, needless anxiety or distress to the recipient. An example of such a law is Section 127 of the UK's Communications Act 2003 which punishes 'grossly offensive messages'. However, even then, prosecutors are issued with guidelines on how to handle such cases and prosecution is only allowed if doing so serves the public interest. To avoid the provisions being misused, the section is limited to cases which go beyond words that are 'offensive, shocking or disturbing; or satirical, iconoclastic or rude; or the expression of unpopular; or unfashionable opinion about serious or trivial matters, or banter or humour, even if distasteful to some or painful to those subjected to it'.[5] No such clear definition of an offensive communication is found in the Computer Misuse Act and no such guidelines to prosecutors have so far been issued.

Sexuality has always been used as an excuse for clamping down on people, as it is a sensitive subject for most members of society. However, this time, this excuse should not be accepted, and Ugandans should see Section 25 of the Computer Misuse Act for what it is: an attempt to stifle the voices of marginalised persons and a continued ploy to deny both sexual minorities and political opponents their rights and freedoms. The Stella Nyanzi case should wake all of us up to the fact that this law can be used against anyone regardless of their position in society. It is thus in the best interests of everyone to oppose it.[6]

4 Constitutional Appeal No.2 of 2002.

5 See The Crown Prosecution Service 'Guidelines on prosecuting cases involving communications sent via social media' available online at http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/ (accessed 15 October 2017).

6 A constitutional challenge against the provision was already launched in the case of *Andrew Karamagi & Robert Shaka v Attorney General*, Constitutional Petition No. 5 of 2016, which is still pending before the Constitutional Court of Uganda. We expectantly await the Constitutional Court 's decision in this matter.

OVERVIEW OF THE ACT

The Computer Misuse Act, 2011: Background and Overview

Adrian Jjuuko
Executive Director, HRAPF

Justine Balya
Legal Assistant, HRAPF

Background

The Computer Misuse Act, No. 2 of 2011 started its life as the Computer Misuse Bill, No. 23 of 2008. The Bill was prepared by the Uganda Law Reform Commission, and tabled before Parliament by the Minister of Information and Computer Technology. It was one of the three laws on computer usage that were later passed by Parliament in 2011. The other two are: The Electronic Signatures Act and The Electronic Transactions Act. These two Acts are concerned with streamlining and regulating electronic economic transactions while the Computer Misuse Act focuses on punishing the use of computers to commit fraud and other crimes.

According to the Memorandum to the Computer Misuse Bill, 2008, the Bill was intended to enable the full utilisation of the opportunities emanating from the rise in the use of Information and Communication Technologies in the country, and as such create a conducive environment that was free of abuse and misuse.[1] The long Title to the Act indeed captures this essence as it shows that the Act was intended to prevent abuse and misuse of information systems by regulating the conduct of electronic transactions, and the safety and security of information transmitted electronically.[2]

This article presents the Act as it stands today, pointing out the salient features of the different parts. It deals with each part of the Act separately:

1 Memorandum to the Computer Misuse Bill, No. 23 of 2008.

2 Long Title of the Computer Misuse Act, 2010.

Part I of the Act

This part contains commencement information and interpretation of terms used in the Act. The Act was to come into force on a date appointed by the Minister. The interpretation section contains various definitions of the key terms used in the Act. A computer is defined in very wide terms to refer to

> ... an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or 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.

This includes smart telephones, laptops, and other such devices. Other terms defined include: access, application, content, data, information, intercept, and program.

Part II of the Act: General Provisions

This part of the Act contains provisions that further explain the meanings assigned to key terms used in the Act, particularly those concerning how data is accessed or modified on a computer. These terms include: 'securing access';[3] using a program;[4] authorised access;[5] references;[6] modification of contents[7] and unauthorised modification.[8]

Part III: Investigations and Procedures

This part of the Act provides for three orders, which can be issued by court in relation to data on computers. These are: the preservation order; the disclosure of preservation order; and the production order. The preservation order is issued at the request of an officer investigating the

3 The Computer Misuse Act, Sec 3.

4 Sec 4.

5 Sec 5.

6 Sec 6.

7 Sec 7.

8 Sec 8.

commission of any offence, to access, preserve or procure any computer data necessary for the investigation. The order is issued where data on a computer is reasonably suspected to be in danger of modification, loss or damage and yet that data is reasonably necessary for the investigation of an offence.[9] The disclosure of preservation order is issued for data that has been preserved to be disclosed to an officer investigating the commission of an offence, no matter how or by whom such data was stored or transmitted.[10] The production order enforces the giving of data on a computer to an investigating officer in a format in which it can be taken away and in which it is visible and legible.[11] The process of obtaining the orders does not give the owner of the data or the persons against whom the order is issued an opportunity to appear in court and show cause as to why the orders should not be issued. They are issued entirely on the basis of what the person applying for them says.

Part IV: Computer Misuse Offences

This part is the crux of the Act, as it puts in place penal measures to punish computer misuse. The offences created can be categorised based on the nature of the offence. There are those concerning fraud and exploitation through computers; those concerning access to computers and interception of communications; and those involving harassment of other persons.

The first category of offences are those involving fraud and exploitation through computers, and these are treated as the most serious offences in the Act. They are punishable by a fine of up to Uganda Shillings 7,200,000 Uganda or imprisonment of up to 15 years, or both such imprisonment and fine. Where the offence involves 'protected computers', life imprisonment can be imposed.[12] Protected computers are computers used for or in connection with national security and diplomatic relations, financial services or banking, communications infrastructure, public utilities, public safety and emergency services.

Electronic fraud is one of the offences created. It is defined as:

> '... deception deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.'[13]

The other offences are: unauthorised modification, which is about acts that impair the operation of the computer generally or access to the computer or any of the programs/data on the computer;[14] unauthorised use or interception of computer services which is defined to include, inter alia, knowingly doing anything on a computer so as to secure access to a computer service without authorisation;[15] unauthorised obstruction of use of a computer;[16] and unauthorised disclosure of access codes.[17]

Another important offence that falls under this category is child pornography. This is defined to include pornographic materials that depict a child engaged in sexually suggestive or explicit conduct; a person appearing to be a child engaged in sexually suggestive or explicit conduct; or realistic images representing children engaged in sexually suggestive or explicit conduct.[18] The acts that constitute the offence include: making pornographic materials available to a child;[19] producing 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; or unlawfully possessing child pornography on a computer.[20]

The second category is about unauthorised access to computers and interception of communications. These are punishable with a fine of 4,800,000 Uganda shillings or imprisonment for a period not exceeding 10 years, or both such imprisonment and fine. This category includes 'unauthorized access' which is about unlawfully adapting, producing, distributing, selling or using a computer program designed to overcome security

9 Sec 9.

10 Sec 10.

11 Sec 11.

12 Sec 20.

13 Sec 19.

14 Sec 14.

15 Sec 15.

16 Sec 16.

17 Sec 17.

18 Sec 23(3).

19 Sec 23(2).

20 Sec 23(1).

protocols, or denying service to a legitimate user.[21] The category also includes 'accessing with the intent to commit or facilitate the commission of another offence';[22] unauthorised use or interception of computer data or service,[23] and unauthorised disclosure of information on a computer.[24]

The third category are offences involving cyber harassment. These are regarded as less serious crimes and are punished with smaller fines and imprisonment of less than five years.

Section 24 criminalises cyber harassment. This is committed when a person uses a computer to: 'make any request, suggestion or proposal which is obscene, lewd, lascivious or indecent'; or to threaten someone with physical injury or harm to their person or property; and knowingly permitting another person to use a computer for any of the purposes listed. The punishment for this is a fine of Uganda shillings 1,440,000 or imprisonment not exceeding three years or both.

Section 25 criminalises offensive communications. Any person who 'willfully and repeatedly uses electronic communication to disturb or attempt to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues' is liable to be convicted under it. It is regarded as a misdemeanor and a convict is liable to a fine not exceeding Uganda shillings 480,000 or imprisonment not exceeding one year or both. It is perhaps the most controversial provision in the Act as its vague and wide-sweeping provisions make it a provision that is easy to abuse and to use to unduly restrict freedom of expression.[25]

The final offence under this category is 'cyber stalking'. This is committed when a person 'willfully, maliciously, and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person's immediate family.' The crime attracts a punishment of Uganda shillings 2,400,000 or imprisonment not exceeding five years or both.

21 Sec 12.

22 Sec 13.

23 Sec 15.

24 Sec 18.

25 For a full discussion of the human rights challenges posed by this provision, see editorial to this issue above.

Attempts to commit an offence are also criminalised, and contrary to the usual practice where these attract a lesser punishment, they are punished the same way as the full offence. Perhaps the reason for this is the conflation of attempts with abetment in section 21.

The Act requires compensation to be ordered in every case where a person is convicted. This a mandatory requirement. The convict is supposed to be ordered to pay the aggrieved party such sum of money, which in the court's opinion is 'just, having regard to the loss suffered by the aggrieved party.' The order of compensation is enforceable under the execution provisions of the Civil Procedure Act.

Part V: Miscellaneous Provisions of the Act

This section contains provisions on enforcement of the Act. These include: the powers of courts to issue search and seizure orders; the evidential value of electronic information; the jurisdiction of the courts under the Act including extra-territorial jurisdiction; and the power of the Minister to amend the schedule to the Act.

For search orders, a magistrate has powers to issue an order for the search of any premises, data or copies thereof that may be reasonably suspected to be necessary, among others, for the investigation of a suspected offence. Once a search order is issued, the police officer can then search and seize any computer system or applications that he/she reasonably believes are concerned in the commission of a crime. Such an officer can demand for information from persons in charge of the computer system or compel service providers to provide information within their technical abilities. It is a crime to hinder or prevent the officer from doing his/her work, and a person found guilty is liable on conviction to a fine not exceeding Uganda shillings 240,000 or imprisonment not exceeding six months or both.[26] The section requires that police officers executing such search warrants 'shall have due regard to the rights and interests of a person affected by the seizure to carry on his or her normal activities.'[27] However, it does not in fact give the person whose data is concerned the opportunity to show cause why their privacy should not be so limited, but merely offers the magistrate the right to issue a carte blanche order of sorts, baring all personal data of any individual before the state upon a mere whim or suspicion.

26 Sec 28(7).

27 Sec 28(6).

It is important to note that the Act gives a timeline within which the seized computer system or application is to be returned and this should not exceed 72 hours, unless an order extending the time has been obtained from court.[28]

Section 29 suspends the rules of evidence that would render electronic evidence inadmissible because it is in electronic form, or because it is not in its original form. Such evidence should also allowed where it is the best evidence that could be obtained in the circumstances. Section 29(7) makes it clear that all other rules of evidence apply without modification.

The Act has extra-territorial application, which means that it applies to anyone regardless of their nationality or their presence in Uganda,[29] provided they were in Uganda at the time of commission of the offence or the program used was based in Uganda at that time.[30]

A Chief Magistrate or Magistrate Grade 1 has powers to listen to any offences under the Act, regardless of what other laws may provide as to sentencing jurisdiction.[31]

Finally, the Minister of Information and Computer Technology has powers to amend the only schedule to the Act, which lays out the value of a currency point.[32] It is surprising that for such a law, the Minister was not given powers to make Regulations for its enforcement.

Conclusion

The Computer Misuse Act, 2011 largely lives up to its promise of enacting provisions aimed at ensuring that computers are not abused or used for fraud. However, some of its provisions depart from the usual rules on punishments for attempted offences; the rules of evidence and those on jurisdiction. Also, it gives wide powers to the police and courts as regards issuance of orders under the Act, and yet it does not give the subject of these orders a chance to show cause as to why they should not be issued. Such provisions are likely to be abused by law enforcement officers.

The punishments, such as mandatory compensatory orders, are deterrent and thus help to reduce on incidences of cybercrime. The provisions on child pornography as well as those on cyber stalking and cyber harassment are wide and deterrent. The provision on offensive communications ought to be removed from the Act as it is vague and also goes against the right to freedom of expression.

The Act is thus a welcome step in the protection of the privacy of personal data stored and shared electronically, as well as protection of the integrity of computer systems and communications, but it also presents enormous potential for abuse in the absence of adequate safeguards protecting the fundamental rights to liberty, administrative fairness, freedom of thought, conscience, opinion, belief and expression as well as press freedom in Uganda.

...it gives wide powers to the police and courts as regards issuance of orders under the Act, and yet it does not give the subject of these orders a chance to show cause as to why they should not be issued. Such provisions are likely to be abused by law enforcement officers.

28 Sec 28(8).

29 Sec 30(1).

30 Sec 30(2).

31 Sec 31.

32 Sec 32.

HUMAN RIGHTS ANALYSIS

The Computer Misuse Act and the Right to Freedom of Expression and Privacy

Susan Baluka
Legal Officer, HRAPF

Introduction

The rights to privacy and freedom of expression are guaranteed in Uganda's Constitution[1] and other regional and international human rights instruments that Uganda is party to. The government of Uganda has made efforts towards creating a legal and policy environment to foster and regulate these rights amidst ever-increasing reliance on technology for information access, sharing and storage. This is evidenced by the wide range of cyber-related laws that have been recently enacted.[2] While such efforts are commendable, the existing cyber laws pose a grave danger to the enjoyment of the online freedom of expression and the right to privacy.[3] One law that requires particular focus is the Computer Misuse Act, 2011. The long title to the Computer Misuse Act stipulates that it is

> 'an Act meant to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment.'[4]

This is a clear indication that the Act was enacted primarily to provide for privacy and data protection rights of internet and computer users. The Act however has provisions that have the potential to infringe upon the right to freedom of expression to an extent that is not in line with domestic, regional and international human rights standards.

This article examines certain key provisions of the Computer Misuse Act 2011 in relation to the right to freedom of speech and expression, as well as the right to privacy.

The Right to Freedom of Expression

Domestic context

Article 29(1) of the 1995 Constitution of the Republic of Uganda stipulates that every individual shall have the right to freedom of expression, which includes the right to freedom of press and other media. This right is not absolute and while it does not have a specific clawback clause, the parameters for its restriction can be found in Article 43 of the Constitution. The Article is to the effect that in the enjoyment of human rights and freedoms stipulated in Chapter Four of the Constitution, no person shall prejudice the rights and freedoms of other individuals or the public interest. The Article further states that public interest shall not permit political persecution or violation of a right beyond what is justifiable in a free and democratic society. The Supreme Court of Uganda in the case of *Charles Onyango Obbo & Andrew Mujuni Mwenda v Attorney General*[5] discussed this limitation and found that the limitation itself, has a further limitation showing clearly that the right has to be given more prominence than the limitation, and the limitation must be justified, and legitimate in order to be in public interest.

The Regional Context

The African Charter on Human and Peoples'

1 See Arts 41, 27 and 29 of the Constitution of the Republic of Uganda, 1995.

2 These include: The Anti-Terrorism Act, 2002; The National Information Technology Authority Uganda Act, 2010; The Regulation of Interception of Communications Act, 2010; The Electronic Signatures Act 2011; The Computer Misuse Act 2011; The Electronic Transactions Act 2011; The Uganda Communications Act 2013; and The Anti-Pornography Act 2014.

3 Collaboration on International ICT Policy in East and Southern Africa (2014), *State of Internet Freedoms in Uganda 2014: An Investigation into Policies and Practices Defining Internet Freedom in Uganda*. Available online at https://cipesa.org/?wpfb_dl=181(accessed on 26 September 2017).

4 The Uganda Gazette, Acts Supplement No. 2 (2011).

5 Constitutional Appeal No.2 of 2002.

Rights (African Charter) also provides for freedom of expression and opinion, as long as such expression is within the limits of the law.[6] The African Charter, limits this right through the general limitation clause in article 27(2). The limitation clause is to the effect that all the individual rights and freedoms recognised in the Charter shall be exercised 'with due regard to the rights of others, collective security, morality and common interest.' The African Commission on Human and Peoples' Rights (African Commission) adopted the Declaration of Principles on Freedom of Expression in Africa. The Declaration affirmed freedom of expression as 'a fundamental and inalienable human right and an indispensable component of democracy.'[7] It further stated that 'Any restrictions on freedom of expression shall be provided by law, serve a legitimate interest and be necessary in a democratic society.'[8] The requirement that the limitation be provided for by law does not simply mean that any law qualifies. It must be a law of general application as the African Commission noted and held in *Constitutional Rights Project and others v Nigeria*.[9] In that case, the military government in Nigeria had made decrees specifically naming the newspapers that were not allowed to operate in Nigeria. The African Commission found this to contravene Article 9 on freedom of expression. On serving legitimate interests, and necessity, the state must show what those interests are why the law is necessary. Here the proportionality test is applied. The extent of the limitation must be proportionate to the interests that have to be protected. In *Independent Journalists Association of Zimbabwe, the Zimbabwe Lawyers for Human Rights, the Media Institute for Southern Africa v Zimbabwe*,[10] the African Commission stated that proportionality is about balancing between the 'protection of the rights and freedoms of the individual and the interests of the society as a whole.'

The Commission stated that

'In determining whether an action is proportionate, the Commission will have to answer the following questions:

- Were there sufficient reasons supporting the action?
- Was there a less restrictive alternative?
- Was the decision-making process procedurally fair?
- Were there any safeguards against abuse?
- Does the action destroy the very essence of the Charter rights in issue?[11]

The notion of proportionality was further discussed by the African Court in *Lohe Issa Konate V Burkina Faso*,[12] where a sentence of 12 months' imprisonment, a fine of USD 2,900 and a compensation fee of USD 7,800 that were imposed against two editors of a weekly newspaper in Burkina Faso for publishing a libelous article against an allegedly corrupt state prosecutor was held to be in contravention of the right to freedom of expression as provided for under Article 9 of the African Charter. The Court reasoned that the sentence was disproportionate to the purpose that the impugned provisions of the Information and Criminal Codes of Burkina Faso sought to serve; which was to protect the honor and reputation of persons working in public offices. The Court found that the provisions were a disproportionate interference with the exercise of the right to freedom of expression, exceeding the bounds of necessity and unanimously ordered Burkina Faso to amend its criminal defamation laws by repealing custodial sentences for acts of defamation. Indeed, following this decision, Burkina Faso has since amended its criminal defamation laws.[13]

Therefore from the above analysis, section 24 and 25 of the Computer Misuse Act have to be justified by the state and a balance made as to whether they are proportionate to the mischief that they seek to address.

6 Art 9(2) of the African Charter on Human and Peoples' Rights.

7 The African Commission on Human and Peoples' Rights 'Resolution on the Adoption of the Declaration of Principles on Freedom of Expression in Africa' Adopted at The African Commission on Human and Peoples' Rights, meeting at its 32nd Ordinary Session, in Banjul, The Gambia, from 17th to 23rd October 2002, Para I(1) http://www.achpr.org/sessions/32nd/resolutions/62/ (accessed 21 October 2017).

8 Above, Para II (2).

9 (2000) AHRLR 227 (ACHPR 1999) Para 44

10 Communication No.297 of 2005.

11 Above. Para 176.

12 Application No.004 of 2013 available online at http://www.ijrcenter.org/2015/02/03/african-court-addresses-freedom-of-expression-in-burkina-faso-in-landmark-judgment/

13 The ACTHPR Monitor, *Protecting the Safety of Journalists: The Role of the African Court* available at http://www.acthprmonitor.org/protecting-the-safety-of-journalists-the-role-of-the-african-court/(Accessed on 22 October 2017).

Additionally, laws that restrict freedom of expression must be clear on which sorts of expressions are limited and which ones are not, and they must not give unfettered discretion to those charged with their execution to restrict freedom of expression.

The International Context

Article 19(2) of the International Covenant on Civil and Political Rights provides for the right to freedom of expression, which includes the right to seek, receive and impart information. As already mentioned, this right can only be restricted for the purpose of respecting the rights and reputations of other individuals, as well as protecting national security, public order and public morals. The Human Rights Committee has stated that the right to freedom of expression extends to both electronic and internet-based platforms.[14] It has further stated that attacks on individuals, including arbitrary arrests, because of the exercise of their right to freedom of opinion or expression are not a justifiable restriction on the right to freedom of expression. Additionally, laws that restrict freedom of expression must be clear on which sorts of expressions are limited and which ones are not, and they must not give unfettered discretion to those charged with their execution to restrict freedom of expression.[15]

The Computer Misuse Act and the aforementioned standards

Section 25 of the Computer Misuse Act creates the offence of offensive communication. The Section is to the effect that any person who wilfully and repeatedly uses electronic communication to disturb the peace, quiet or right to privacy of any other person, with no purpose of legitimate communication and whether or not a conversation ensues, commits a misdemeanor, and is liable on conviction to a fine not exceeding 24 currency points and 1 year's imprisonment in the alternative. This provision does not provide clear guidance as to what communication amounts to 'disturbing of the peace,' neither does it distinguish between legitimate and illegitimate communication. As such, the provision gives leeway to law enforcement officials to apply their individual interpretations on whether a communication is illegitimate and amounts to disturbance of the peace. This is in contravention of aforementioned principles that have been enunciated by the Human Rights Committee.[16]

The danger posed by this provision was demonstrated when it was used to arrest and prosecute Dr. Stella Nyanzi, a human rights activist that ardently criticised President Museveni, for repeatedly using the social media platform of Facebook to post messages that were allegedly meant to 'disturb the peace of the president'.[17] By not clearly defining what amounts to disturbance of the peace and illegitimate communication, Section 25 of the Computer Misuse Act gives unfettered discretion to law enforcement officials to unjustifiably restrict individuals' right to freedom of expression and subject them to arbitrary arrest, contrary to the spirit of Article 19 of the International Covenant on Civil and Political Rights and Article 29(1) of the 1995 Constitution of the Republic of Uganda.

The non-compliance of Section 25 of the Computer Misuse Act with the standard of certainty and clarity as a key feature of legislation that limits the right to freedom of expression can further be demonstrated in the decision of the Constitutional Court in *East Africa Media Institute*

14 Human Rights Committee (2011), *General Comment No. 34 to Article 19 of the International Covenant on Civil and Political Rights*, para 23, available online at http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (Accessed on 27 September 2017).

15 Above, para 15.

16 Above.

17 The Guardian, 23rd April 2017, *How Insults and Campaign Over Sanitary Towels Landed Activist in Jail*, accessed at *https://www.theguardian.com/world/2017/apr/22/activist-uganda-president-buttocks-jail-stella-nyanzi* (Accessed on 27 September 2017).

SOURCE: https://www.shutterstock.com

and Andrew Mwenda v Attorney General[18], where similarly broad and vague provisions of Sections 39 and 40 of the Penal Code Act creating the offence of sedition were held to be too vague to warrant a justifiable limitation of the right to freedom of speech and expression. Section 25 of the Computer Misuse Act is essentially a recurrence of the nullified sedition provisions, the vagueness of which was exploited by government to wantonly subject individuals that voiced dissenting and critical opinions and issues against it to criminal prosecution.[19]

Section 24 of the Computer Misuse Act also makes it an offence for an individual to use a computer to make a request, proposal or suggestion that is obscene, lewd, lascivious or indecent. From the onset, this provision would be within the protection of public morals as an exception to observance of the right to freedom of expression. However, the 'morals' exception is not to be unfettered.[20] Any limitation must be within what is necessary and justifiable in a free and democratic society.[21] The broad criminalisation of obscene, lewd, lascivious and indecent suggestions, proposals and requests under Section 24 of the Computer Misuse Act, without specifying the circumstances under which it is prohibited leaves room for it to be applied arbitrarily to limit the right to freedom of expression.

Additionally, as regards the principle of proportionality, while both Sections 25 and 24 of the Act seek to protect the quiet enjoyment of various forms of electronic media by their users, such an aim, when juxtaposed against the right to freedom of expression in a free and democratic society, does not warrant the placing of criminal sanctions on communication that some individuals may or may not find offensive. Indeed, as pointed out by the African Court in *Lohe Issa Konate V Burkina Faso*,[22] criminal sanctions are not a justifiable limitation on the exercise of the right to freedom expression. The balance between the individual right to privacy and the right to freedom of expression is sufficiently catered for by civil law in the torts of defamation and nuisance.

The Right to Privacy

Domestic Context

Article 27 of the 1995 Constitution of Uganda provides for the right to privacy of information wherein it stipulates that no person shall be subjected to interference with the privacy of

18 Consolidated Constitutional Petitions No. 12 of 2005 and No. 3 of 2006

19 Human Rights Watch *A Media Minefield: Increased Threats to Freedom of Expression in Uganda* (2010) available online at https://www.hrw.org/report/2010/05/02/media-minefield/increased-threats-freedom-expression-uganda (Accessed on 22 October 2017).

20 Article 19 *Freedom of Expression Handbook* (1998) available online at https://www.article19.org/data/files/pdfs/publications/1993-handbook.pdf (Accessed on 27 September 2017).

21 Art 43(2)(c) of the Constitution of the Republic of Uganda, 1995.

22 n 12 above.

their correspondence, communication or other property. The right to privacy, as are other non-derogable rights provided for in the bill of rights, is subject to limitation on grounds of protection of the rights of other individuals and the public interest, as stipulated in Article 43 of the Constitution. In Uganda, this right has mainly been limited on the basis of protecting the public interest, specifically, the need to ensure national security.[23] According to the Supreme Court in *Attorney General v Maj. General David Tinyefuza*[24], an assertion that the infringement upon the right to information is necessary to ensure national security is not sufficient, as the state must adduce evidence to prove it. While this case was primarily about the right to access to information, in the absence of elaborate case law on the right to privacy of communication and information in Uganda, its *ratio decidendi* is very helpful in demonstrating that infringement on a right by the state, including the right to privacy, on grounds of national security, is only permissible where evidence of the necessity of such infringement to the protection of national security is adduced by the state.

Regional and International Context

While at the regional level, the African Charter does not address the right of the privacy of communication, it has been addressed at the international level by the International Covenant on Civil and Political Rights (ICCPR), as well as the Committee on Civil and Political Rights.

Article 17 of the ICCPR stipulates that the no one shall be subjected to unlawful and arbitrary interference with their privacy, family, home or correspondence. The Committee on Civil and Political Rights offers great guidance on what amounts to 'unlawful and arbitrary interference.' According to the Committee, unlawful interference with the right to privacy is that which is not provided for by law, while arbitrary interference is that which may be provided for by law, but is not in line with the objectives of the ICCPR and is unclear and unreasonable in the circumstances.[25]

Reasonableness has been interpreted by the Human Rights Committee in ***Toonen v Australia***[26] to mean that any interference with privacy must be proportional to the end sought and must be necessary in the circumstances of any given case.

The Computer Misuse Act and Domestic, Regional and International Standards on the Right to Privacy

Section. 9 of the Computer Misuse Act stipulates that an investigating officer may apply to court for an order to preserve data that he or she reasonably believes to be in danger of getting lost or modified. According to subsection 2, data includes subscriber information. The danger with this provision is that, contrary to the constitutional requirement that a right can only be limited according to what is acceptable and demonstrably justifiable in a free and democratic society, it does not clearly address the issue of the relevance of the data that is to be the subject of the court order to the case being investigated. This gives leeway to the investigating officer to intercept personal communication and correspondences of subscribers, even in circumstances where it is not justifiable.

Section 10 of the Act provides for the application of an order for disclosure of data that had been preserved by the investigating officer. The danger with this provision is that it is not clear on the persons or authorities to whom such information is to be disclosed, and what the envisioned purpose of the disclosure will be. While clause (b) of the Section makes reference to interpretation of data as a ground for disclosure, it does not clearly make the linkage as to the ultimate objective of such interpretation. This again leaves room for violation of the right to privacy of the subscribers, whose personal information may be disclosed to unauthorised persons, and without good cause.

Conclusion

As evidenced from its long title, the enactment of the Computer Misuse Act was well intentioned in as far as protection of individual rights of computer and Internet users, as well as data protection are concerned. Unfortunately, the Act has provisions that are too broad and do not provide for specific and well-defined restrictions on the right to freedom of expression and privacy. As such, there is a definite need to have most of the provisions in the Act amended to bring them in line with domestic, regional and international standards on information and expression rights and freedoms.

23 K Mayambala, *Phone Tapping and the Right to Privacy in Uganda* (2008) accessed at http://www.bileta.ac.uk/content/files/conference%20papers/2008/Phone-tapping%20and%20the%20Right%20to%20Privacy%20[Ronald%20Kakungulu].pdf (Accessed on 24 October 2017).

24 Constitutional Appeal No. 1 of 1997.

25 Committee on Civil and Political Rights (1988), *General Comment No.16 on the Right to Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, paras 3-4 accessed at http://www.refworld.org/docid/453883f922.html (Accessed on 24 October 2017).

26 Communication No. 488 of 1992.

FEATURE

In kindred company: The Computer Misuse Act and the other vague and broad laws that threaten the rights of sexual minorities

Joaninne Nanyange
Ag. Deputy Executive Director, HRAPF

Introduction

The Computer Misuse Act, with its vague and overly broad provisions, joins ranks with a number of laws in Uganda that suffer the same deficiency. While some laws with ambiguous provisions have existed since colonial times, the most recent laws have been strategically enacted over the past decade or so with the specific intention of reducing dissent, criminalising diversity, limiting free thought and stifling opposing voices. These vague laws however have the effect of restricting the rights of marginalised persons, particularly sexual minorities, much more than other persons. This article puts into context the vague provisions of the Computer Misuse Act by showing how it simply joins the other laws to further restrict the rights of sexual minorities. It analyses some of the laws in Uganda that contain vague provisions, which have been used or have the potential to be used discriminately against marginalised persons. The focus will be on sexual minorities as they face the harshest marginalisation because of prejudices, and there are specific laws that attempt to criminalise their conduct.

Vagueness and broadness: A conceptual analysis

Vagueness and broadness of laws are two related but different concepts, with different meanings and different framings. The two concepts of 'void for vagueness' and 'void for overbreadth' help to distinguish them:

The Void for vagueness Doctrine

Vagueness of criminal laws in Uganda is dealt with under Article 28(12) of the Constitution, which provides that except in cases of contempt of court, no person shall be convicted of a criminal offence unless that offence is defined and a punishment prescribed by law. This is **the 'Void-for-Vagueness' Doctrine.**

Article 28(12) has however not been fully interpreted in Ugandan jurisprudence and legislation, and therefore the 'void-for vagueness' doctrine has not fully taken root. As a result, many vague provisions remain on the law books and are used to prosecute people despite Article 28(12). This is what the state has exploited to further ostracise already marginalised groups.

In the United States legal system, the doctrine of 'Void-For-Vagueness' has been developed extensively. The doctrine, in as far as the United States is concerned, is derived from their due process clauses of the fifth and fourteenth amendments to the US Constitution that require criminal laws to be drafted in language that is clear enough for the average person to comprehend.[1] The doctrine is to the effect that if a person of ordinary intelligence cannot determine which persons are regulated, what conduct is prohibited, or what punishment may be imposed under a particular law, then the law will be deemed unconstitutionally vague. The void-for-vagueness doctrine has four underlying principles, which will be discussed in turn.[2] These tested principles can be extrapolated to Uganda's context.

1 AE Goldsmith 'The Void-For-Vagueness Doctrine in the Supreme Court, Revisited' 30 *American Journal of Criminal Law* (2003) 282; Encyclopedia, American Law and Legal Information 'Void for vagueness doctrine' available online at http://law.jrank.org/pages/11152/Void-Vagueness-Doctrine.html (accessed 20 October 2017).

2 As above.

First, it requires legislators and government to distinguish between conduct that is lawful and that which is unlawful. This principle exists to ensure that people are given adequate notice of what conduct is criminalised and what conduct is not. When the populace is given adequate notice, they know how to conduct themselves within the legal framework. Vague and unclear laws that do not give people fair warning and notice become a trap for marginalised groups that suffer under societal prejudices.

Second, the doctrine requires that laws are precise, clear and discernible not just to the people that are required to obey them, but also to those that are required to enforce them.[3] This is intended to curb the arbitrary and discriminatory enforcement of such laws. In a study conducted by Human Rights Awareness and Promotion Forum in 2016 for example, it was found that 'vagrancy offences' in Uganda are mainly enforced against marginalised groups like LGBTI persons, sex workers and drug users.[4] Such laws give enforcement officers wide discretion to implement the law as they think fit. When such officers interface with groups of persons that are marginalised and suffer prejudice, they exploit the vagueness of the provisions and enforce the laws discriminately.

Third, the doctrine requires judicial officers not to apply vaguely worded laws.[5] This principle is to the effect that if such laws are to be applied by courts and tribunals, judicial officers should give them very narrow interpretations. It further provides that those that are too vague to be narrowly interpreted by judicial officers should be struck down as unconstitutional.

Fourth, the doctrine cautions against vague laws affecting the enjoyment of rights.[6] Since vague and ambiguous laws create uncertainty as to what conduct is prohibited and what is not, they have the effect of creating self-censorship among citizens, who are conscious that they might engage in something that could be interpreted as criminal. Additionally, the wide discretion given to law enforcers by vague laws creates an opportunity for them to use these laws to clamp down on the legitimate enjoyment of rights. Such laws have for example been used to violate the right to liberty of marginalised groups in Uganda through arbitrary arrests and rights to freedoms of association and assembly through police raids on legitimate events and organising.

...marginalised and unwanted populations bear the brunt of vague and ambiguous laws. ...some of these populations include drug users, sex workers, LGBTI persons, petty traders, market vendors, unemployed and homeless persons, street children and political critics.

As already noted, marginalised and unwanted populations bear the brunt of vague and ambiguous laws. In Uganda, some of these populations include drug users, sex workers, LGBTI persons, petty traders, market vendors, unemployed and homeless persons, street children and political critics. The reason for this is that sometimes the typical behavior or characteristics of unpopular groups (such as unemployed or homeless persons) are not criminalised and yet society wants to use the law to repress them or remove them from the public eye. In many cases where the actions of undesirable minorities are criminalised, the offences they could be charged with are hard to prosecute and prove as in the case of sexual minorities. Enforcers subsequently resort to the vague and broad laws that give them wide discretionary powers to decide what conduct is prohibited.

The over-breadth doctrine

This doctrine is by and large related to the void-

3 Goldsmith (n 1 above) 285.

4 See Human Rights Awareness and Promotion Forum '*The Implications of the Enforcement of 'Idle and Disorderly' Laws on the Human Rights of Marginalised Groups in Uganda*' 2016

5 Goldsmith (n 1 above) 285.

6 For a discussion on the level of certainty which criminal laws were historically required to provide, see CD Lockwood 'Defining indefiniteness: Suggested revisions to the Void for Vagueness Doctrine' 8 *Cardozo Public Law, Policy and Ethics Journal* (2009) 171-2.

SOURCE: https://www.shutterstock.com

for-vagueness doctrine. Over-breadth however concerns offences that sweep up into their prospective net both constitutionally protected and constitutionally unprotected activity.[7] As developed in the United States, this doctrine is mainly used against provisions or laws that are so broad that they extend to activities and rights that are protected by the constitution.[8]

This doctrine has been explored in the Ugandan case of *Charles Onyango Obbo and Andrew Mwenda v Attorney General*[9] where the appellants challenged section 50 of Uganda's Penal Code Act that created the offence of publication of false news. In declaring the section unconstitutional, Uganda's Supreme Court noted that the section was too broad and capable of very wide application and the effect of this was to perpetually place the affected persons in a dilemma over what was criminalised and what was not. The court noted that the section would have the effect of either some people taking the plunge and getting prosecuted or create self-censorship among those that were cautious enough to avoid prosecution. In any case, the court noted that the effects were injurious to enjoyment of the freedom of expressions and democracy. Additionally, the court also noted that the broadness of the section had the effect of giving prosecutors unfettered discretion to determine, from time to time, what was criminalised and what was not, which cannot be acceptable or justifiable in a free and democratic society.

The *Onyango Obbo case* highlights the most glaring shortcomings of broad laws, namely they put the public in a dilemma as to what conduct is criminalised and give law enforcers unfettered discretion to make that decision. As noted, this either leaves many people susceptible to persecution in the form of prosecution, or creates a chilling effect on the public where people avoid engagement in legitimately protected conduct because they are wary of being caught up in the ambit of the criminal provisions. Needless to emphasise, both situations are catastrophic to the enjoyment of rights and are claw backs to the aspirations of a free and democratic society.

It should, however, be noted that courts acknowledge the fact that almost all laws affect conduct that is ordinarily protected in Bills of Rights, and that striking down every law that seems to affect protected conduct would be problematic. Courts have therefore created space to allow existence of laws that are written in general terms by introducing the substantiality test.[10] In essence, this test requires that for a law to be struck down as overly broad, one must show that it not only affects conduct that is protected, but that it affects such conduct in a substantial manner as to make the protection of the conduct illusory.

Vague and overly broad laws in Uganda and their impact on Sexual minorities

The following laws contain vague and/or overly broad provisions that disproportionately affect sexual minorities. They are classified between those that directly affect sexual minorities and those that indirectly affect sexual minorities:

7 Rottenstein Group 'What does it mean when a law is "void for vagueness" or "overbroad"? http://www.rotlaw.com/legal-library/what-does-it-mean-when-a-law-is-void-for-vagueness-or-overbroad/ (accessed 23 October 2017)

8 As above.

9 Constitutional Appeal No. 2 of 2002.

10 *Ashcroft v Free Speech Coalition* 535 U.S 234 (2002).

Vague and broad laws that directly affect sexual minorities

Unnatural Offences under the Penal Code Act

The Penal Code Act is Uganda's cardinal criminal law. Sections 145 and 146 of the Penal Code Act criminalise carnal knowledge against the order of nature, which has been (mis)interpreted as criminalising homosexuality.[11] This common misunderstanding of this provision by law enforcement officers and various duty bearers is not accidental. It is a result of the vagueness of the provision. The provision does not define the term 'order of nature' and neither does the Act. As a result, the provisions are often subjectively interpreted and what 'against order of nature' means more often than not, depends on whom you ask. The provisions have not been the subject of extensive litigation. However, a few cases have shed light on its meaning. In the case of *Kasha Jacqueline Nabagesera & Others v Rolling Stone Newspaper & Another*[12] the judge stated that section 145 is limited to sexual acts and not identity and orientation. However, in the subsequent case of *Kasha Jacqueline Nabagesera & Others v Attorney General & Another*,[13] the High Court held that holding a skills training workshop for LGBTI persons is against the law as it amounts to conspiracy to commit the offences created in sections 145 and 146. This case distinguished the earlier decision on the basis that it dealt with different circumstances. The first interpretation is the one employed by organisations working to protect the rights of LGBTI persons, for example HRAPF,[14] while some state agencies such as the Uganda Registration Services Bureau (URSB) choose to use the second wider interpretation to refuse incorporation of organisations whose names or objectives explicitly mention working with sexual minorities.[15]

From the above, the position of the law remains vague. This vagueness, coupled with the prevalent homophobia in Uganda, continue to be leading causes of violations of rights of LGBTI persons.

The Anti-Homosexuality Act, 2014 (now nullified)

The Anti Homosexuality Act was passed by Uganda's Parliament in December 2013 and signed into law by the President in February 2014. The Act remains Uganda's greatest attempt at comprehensively and directly criminalising homosexuality. As previously discussed, the current criminal framework only criminalises carnal knowledge against the order of nature. The Anti-Homosexuality Act expressly criminalised same sex sexual conduct and extended to aiding and abetting homosexuality and what was termed 'promoting homosexuality'. In March 2014, the Civil Society Coalition on Human Rights and Constitutional Law filed a petition in Uganda's Constitutional Court[16] challenging the constitutionality of some of the provisions of the Act and the manner of its passing (that it was passed without quorum). The Constitutional Court heard the case and on 1st August 2014, declared the Act unconstitutional as it had been passed without quorum. Attempts to re-table a similar Bill in Parliament have not materialised. The Act is currently not in force but its effects remain.

Sections on aiding and abetting and promoting homosexuality were unconstitutionally broad in as far as they prohibited legitimate and constitutionally protected work like health service provision and human rights advocacy.

11 Human Rights Awareness and Promotion Forum and the Civil Society Coalition on Human Rights and Constitutional Law *Protecting 'Morals' by Dehumanising Suspected LGBTI Persons? A Critique of the Enforcement of the Laws Criminalisng Same-sex Conduct in Uganda* (2013) 43.

12 Miscellaneous Cause No. 163 of 2010.

13 High Court Miscellaneous Cause No. 33 of 2012.

14 See Human Rights Awareness and Promotion Forum (HRAPF) *A Guide to the Normative Legal Framework on the Human Rights of LGBTI Persons in Uganda* 25.

15 The case of *Frank Mugisha & Others v URSB* High Court Miscellaneous Cause No. 96 of 2016.

16 Constitutional Petition No. 008 of 2014.

The environment in Uganda is permeated with an undeniable phobia for LGBTI persons, and since the early 2000s when the debate on homosexuality truly gained traction in Uganda, the general feeling has been that there is not enough restriction in the law to 'curb' homosexuality. This feeling manifested itself in various events occurring between 2005 and 2014 in Uganda, both on the legislative and law enforcement fronts and in social circles in Uganda, which culminated in the passing of the highly publicised and controversial Anti-Homosexuality Act.

During its existence, the law posed a grave threat to the very lives of suspected LGBTI persons in Uganda as it occasioned such intense discrimination and homophobia. Among others, the law created offences of 'attempt to commit homosexuality',[17] 'aiding and abetting homosexuality'[18] and 'promotion of homosexuality.[19] Sections like attempt to commit homosexuality were so vague in nature in as far as they did not criminalise specific conduct. Sections on aiding and abetting and promoting homosexuality were unconstitutionally broad in as far as they prohibited legitimate and constitutionally protected work like health service provision and human rights advocacy. As a matter of fact, during the existence of the Act, organisations were raided[20] and suspended, [21] individuals arrested and a number of other violations committed. If the law had stood the test of constitutional muster, these provisions would have posed a grave danger to the lives and well-being of LGBTI persons and would have hampered service provision to them. Even when the law was annulled, its halo remains and is exhibited in instances when LGBTI persons are arrested and charged with offences under it, and the persistence of 'promotion of homosexuality/ recruitment into homosexuality' propaganda by anti-gay groups and activists. The effects of this law remain visible in the enforcement of existing legislation, and in the development of new legislation,[22] which are being used to clamp down enjoyment of rights by sexual minorities.

SOURCE: https://www.shutterstock.com

Laws that indirectly affect sexual minorities

The Non-Governmental Organisations Act, 2016

The NGO Act of 2016[23] is the law that governs the registration and operation of NGOs in Uganda. Among others, the Act puts special obligations on all NGOs to refrain from engaging in activities that are prejudicial to the 'security and laws of Uganda' and the 'interests and dignity' of the people of Uganda.[24] As expected, the Act does not define 'security', 'interests' or 'dignity' of Ugandans. The Act does not state the status of the 'special obligations' and what would happen if an organisation breaches any of the obligations.[25] These obligations seem to be core requirements for organisations operating in Uganda and since there is no guidance as to their effect or implications, law enforcers can implement them

17 Sec 4.

18 Sec 7.

19 Sec 13.

20 https://2009-2017.state.gov/r/pa/prs/ps/2014/04/224431.htm (Accessed 23 October 2017).

21 https://76crimes.com/2015/01/23/uganda-refugee-project-survives-anti-gay-attacks-of-2014/ (Accessed 23 October 2017).

22 For example some provisions of the NGO Act 2016 were included to curb against organisations that 'promote homosexuality' since the Anti-Homosexuality Act was annulled.

23 See Human Rights Awareness and Promotion Forum Legal Analysis of the NGO Bill, 2015 (2016) and Human Rights Awareness and Promotion Forum 'The Likely Implications of the Non-Governmental Organisations Act 2016 on Marginalised Groups' 3 *The Human Rights Advocate* (2016) for detailed discussions of the provisions of this law, available online at www.hrapf.org.

24 Sec 44 of the Act lays out the special obligations of NGOs.

25 Sec 40(1)(d) provides that an organisation commits an offence that engages in any activity prohibited by the Act. However, it is debatable whether the breach of a special obligation would amount to engaging in an activity prohibited by the Act.

in any way they deem fit.

Considering the backdrop against which the Act was enacted, its overly broad and almost unenforceable provisions create a potential threat for organisations that work on unpopular issues or with unpopular persons such as sexual minorities. These provisions could be used to close down organisations or even impose criminal liability on directors of such organisations. The provisions are too vague for a person to understand what is really prohibited and too broad to the extent that they substantively limit legitimately protected rights of association, assembly and expression. While the impact of these sections has not yet materialised with sexual minorities, the Act is already being used to close down operations of organisations involved in political dissent and it is a matter of time before this enforcement is extended to organisations working with unpopular populations like sexual minorities.

The Public Order Management Act, 2013

This Act was adopted to regulate the exercise of the freedom to assemble and to demonstrate together with others in a peaceful and unarmed manner and to petition in accordance with Articles 29(1)(d) and 43 of the Constitution.[26] The Act however has been unnecessarily restrictive and has led to the arbitrary limitation of the freedoms it sought to operationalise. One of the reasons for this is that some of the Act's provisions are so vague and ambiguous and grant extremely wide discretionary powers to implementing officers to interpret the Act as they deem fit.

Section 4 defines a public meeting to mean 'a gathering…held for the purposes of discussing…a matter of public interest'. The Act however does not define what would amount to a matter of public interest, yet this definition determines the types of meetings that should be subjected to the requirements laid down in the Act. Any matter can be said to be a matter of public interest, depending on the implementing officer. It should be noted that under the Act, there are restrictions on the holding of meetings that qualify as public meetings, with the Act establishing requirements of notification of the police three days before such a meeting is held,[27] and giving powers to law enforcement authorities to refuse the holding of such meetings. Since such restrictions substantively affect the enjoyment of protected freedoms, it would be prudent to ensure that the enabling law is as precise as possible regarding the extent to which the law can be applied.

While the section goes ahead to provide for what a public meeting is not, this list is not all-inclusive, as the legislature could not be reasonably expected to foresee all types of meetings. What would be easier would be a much more precise definition of what a public meeting is, and not what it is not. The effect of the ambiguous definition of a public meeting is that it leaves the decision of which meetings should be brought under the operation of this law and which ones should not be in the hands of law enforcement officers. As discussed above on the populations that often bear the brunt of such laws, it is marginalised groups that are likely to be affected by such wide discretion.

In August 2016, a beauty pageant held during the LGBTI pride week was raided and stopped on the grounds that it was a public meeting and that the requisite notice had not been sought from police. From the definition given in the Act, one could say that this was a social event that excluded it from being a public meeting, or that the event was never intended to discuss any matter of public interest, as it was merely a beauty pageant for the pride celebrations. However, all these arguments could not be validly made as one can not tell for sure whether this was a public meeting or not. Even if one could, the law leaves the discretion with the enforcement officer to decide what is a public meeting and what is not. As a result, organisers and activists were arrested at that event and brutalised, simply because the

26 Sec 2.

27 Sec 5.

officers had the power to decide whether the Public Order Management Act applied or not. This law therefore presents high potential for abuse, especially against criminalised and prejudiced minorities like LGBTI persons and sex workers.

The Companies Act, 2012

Many organisations working on issues of sexual minorities have up to now elected to register as companies limited by guarantee. Even under the new NGO regime, all organisations seeking to operate as NGOs will be required to first be incorporated as companies limited by guarantee. The Companies Act gives the Registrar of Companies powers to refuse the reservation of a company name that is regarded as undesirable.[28] The Act does not define what 'undesirable' means and neither do the Regulations to the Act. This provision gives the Registrar much discretion to decide which name is desirable and which one is not. This provision has been used before to refuse the reservation of the name Sexual Minorities Uganda (SMUG), on grounds that the name was undesirable.

The reasons given by the Registrar of Companies for deciding that the name 'Sexual Minorities Uganda' was undesirable was that the objectives of the organisation showed that it intended to work with LGBTI persons whose perceived behaviour is criminalised under section 145 of the Penal Code Act. Although the case is currently in the High Court pending determination,[29] it was difficult to contest the legitimacy of this decision because the Act does not provide clear guidance to the Registrar's exercise of these powers. It is important to note that failure to reserve a name puts a halt to the incorporation exercise of an organisation. While a name can be changed, the decision made in the SMUG case was not merely based on a name, but rather on the objectives of the organisation. The refusal to reserve the name based on the objectives of the organisation was essentially a refusal to incorporate the organisation, except if the organisation changed its objectives.

Due to the wide discretion granted under the provision, it was used by the Registrar of Companies to not only refuse the reservation of the name of an intending organisation, but also essentially to stop the incorporation of an organisation. This interpretation would arguably go beyond the application of section 36, but this would be a question of interpretation for the courts to determine as the section is quite broad and undefined. Such a section has affected, and carries the risk of continuing to affect, the rights of association for organisations intending to work with unpopular groups like sexual minorities.

The Vagrancy and nuisance laws in the Penal Code Act

The vagrancy and nuisance laws are found in sections 167 and 168 of the Penal Code Act. These provisions create the offences of being idle and disorderly and being a rogue and vagabond respectively. The offence of being idle and disorderly among others criminalises any person who publicly conducts himself or herself in a manner likely to cause a breach of the peace and any person who in any place solicits or loiters for immoral purposes. The offence of being a rogue and vagabond on the other hand criminalises a suspected person who has no visible means of subsistence and cannot give a good account of himself or herself and persons found wandering in or upon or near any premises or in any road or highway or any place adjacent thereto or in any public place at such time and under such circumstances as to lead to the conclusion that such person is there for an illegal or disorderly purpose, among others.

Many sexual minorities who come into conflict with the law are charged with these offences instead of the actual offences for which they are arrested i.e. suspicions of homosexuality (carnal knowledge against the order of nature) and sex work. In a few instances, particularly for transgender women, police have used the offence of being a common nuisance, which is created under section 160.[30] This section provides that any person who does an act not authorised by law or omits to discharge a legal duty and thereby causes any common injury, or danger or annoyance or obstructs or causes inconvenience to the public in the exercise of common rights commits an offence of common nuisance. In a study conducted in 2016, it was found that these offences were generally favoured by the Uganda Police Force for charging and prosecuting suspected sexual minorities because they were broad enough to cover a wide range of innocuous behavior and were far easier to prove than the unnatural offences or prostitution charges.[31]

It has indeed been shown that convictions on

28 Sec 36 of the Act.

29 The *Frank Mugisha Case* (n 16 above).

30 HRAPF (n 14 above) 26.

31 See Human Rights Awareness and Promotion Forum *The Implications of the Enforcement of 'Idle and Disorderly' Laws on the Human Rights of Marginalised Groups in Uganda* (2016) 25; Also see *Lanzetta v New Jersey* 306 US 451.

SOURCE: https://www.shutterstock.com

charges of having carnal knowledge against the order of nature or prostitution are almost impossible to obtain, so in most cases suspected sexual minorities will be charged under these vagrancy laws.[32] The offences are broad enough to cover conduct as harmless as moving around, but not so broad as to make it impossible to prosecute cases under them. The implication this has had is that sexual minorities in Uganda essentially have no right to liberty and freedom of movement except as granted by the arresting officer. Also, the provisions have been used to extort money from sexual minorities, punish them for their behaviour and subject them to unlawful detention. These provisions are a classic example of laws that offend the over-breadth doctrine discussed above, as they limit conduct that is protected by Uganda's Constitution in Article 23 in a substantial and unjustified manner.

Conclusion

The Computer Misuse Act is part of a series of laws that seek to limit the rights of unpopular minorities through legal sanctions based on provisions that are far too vague and broad to pass constitutional muster.[33] It has therefore become necessary to examine the effect of this law in the general scheme of such legislations and the likely implications of its enforcement on the basic rights of marginalised persons in Uganda. With the annulment of the Anti-Homosexuality Act, continued absence of the tabling of a new law akin to the Anti-Homosexuality Act and the apparent reluctance for the offences on sex work to be enforced, vague and broad offences have become the most obvious choice for law enforcers when dealing with unpopular populations like sexual minorities. They cast a net wide enough to cover a broad range of conduct, and do not present considerable challenges to prosecution, as they require minimal evidence. However, their continued selective enforcement is a cause for concern as it grossly violates the human rights of targeted populations. Advocacy efforts should be engaged in to ensure that these laws are amended, or at the very least, that they are not enforced in a manner that is deliberately discriminatory, opportunistic and marginalising to minority groups.

The Computer Misuse Act is part of a series of laws that seek to limit the rights of unpopular minorities through legal sanctions based on provisions that are far too vague and broad to pass constitutional muster.

32 See HRAPF and CSCHRCL (n 11 above) 21-2.

33 Art 28(1) of the Constitution, *Salvatori Abuki & Another v Attorney General*, Supreme Court Case No. 1 of 1998.

COMPARATIVE PERSPECTIVE

Picking a leaf from other jurisdictions: What Uganda can learn from recent developments on offensive communications laws in India, Tanzania and the UK

Edward Ssemambo
Lawyer,
Kiiza, Tumwesige & Ssemambo Advocates

Introduction

The use of computers has undoubtedly made communication and research easier, connection simpler, business cheaper, security stronger and data storage cheaper. It has promoted entertainment, education, and made history more accessible in real time with just the click of a button. The international network is generally linked to computers and other computer based devices such as smart phones and smart televisions.

Whereas these gadgets have made life seem much easier, they have also brought up a new era of virtual crime which was probably never envisaged in the earlier years. The ability to achieve what one wants no matter where they are without having to be physically be present has made it easy for certain unique crimes. Various countries' legislatures have come up with legislation to try and curb such crimes and deter persons from misusing computers.

In Uganda the Computer Misuse Act, 2011 was enacted purposely to handle, among others, crimes that arise from the use of the computer.[1] The Act defines a computer to mean an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or 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.[2] It should be noted that the computer is merely a means or a platform for committing offences already prohibited by other legislations; and most if not all these offences predate the invention and adoption of computers and social media in Uganda.

In this era of the increasing access to the internet and access to computers and mobile devices, Section 25, which criminalises 'offensive communications', is of particular interest as it can essentially affect the diverse social media platforms including facebook, twitter, linked-in, and google. These modes have been used to communicate, do business, and generally to influence society and any law which curbs the use of these mediums have to be assessed critically. This article considers Section 25 of the Act, in light of similar provisions regulating offensive communication in other jurisdictions in various parts of the world.

A comparison on the restriction of offensive communication

The Act of 2011 creates several computer misuse offences,[3] their punishments, jurisdiction, investigation procedure, admissibility of evidence and the burden of proof among others. It applies to both natural and artificial persons such as corporations.

Under Section 25, it's an offence to willfully and repeatedly use electronic communication to disturb or attempt to disturb the peace, quiet or right to privacy of any person with no purpose of legitimate communication whether or not a conversation ensues. The person found guilty commits a misdemeanor and upon conviction the penalty is either a fine not exceeding Ug.Shs 480,000 (Uganda Shillings Four Hundred Eighty Thousand) or

1 The purpose of the Act is to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters.

2 See Sec 2.

3 All of which are felonies save for one.

imprisonment not exceeding one year or both.

It should be noted that, just like it is in other parts of the world especially the developing world, the internet has proved to be the most cost effective, easy entry way of sharing ideas and information. In fact, computers are increasingly replacing the traditional means of communication. In light of the broad and vague nature of Section 25, communication via the internet has to be done with caution not to amount to a breach of the law. This Section is comparatively assessed in light of similar laws in the United Kingdom, India and Tanzania. These countries were selected because they share a common heritage of influence of British Law with Uganda and, though their socio-political contexts vary, are appropriate comparators to Uganda. Their levels of development differ, with the UK being the most developed, followed by India and then Tanzania, which is almost comparable to Uganda in terms of development, and consequently computer access and penetration. The countries will be discussed in this order.

The United Kingdom

The United Kingdom (UK) has many laws that are sensitive to human rights. The UK's criminal law provision against offensive communication is found in the Communications Act of 2003 which in Section 127(1)(a) provides that 'a person is guilty of an offence (a) if he sends by means of a public electronic communications network a message or other matter that is grossly offensive or of an indecent, obscene or menacing character'. The Malicious Communications Act 1988[4] furthermore, under Section 1 provides that a person is guilty of an offense if they send an electronic communication or article of any description which is grossly offensive and if their purpose in sending it is that it should cause distress or anxiety to the recipient.

Laws against offensive communication have a direct impact on the right to freedom of expression, and for this reason the standard in relation to the offense is high, requiring that the statement must be 'grossly offensive'. The UK is party to a number of international instruments including The European Convention on Human Rights (ECHR) whose provisions on the right to freedom of association clearly protect expression of views that may shock, annoy, disturb or offend the deeply held beliefs of others.[5] The term 'grossly offensive' has also been defined narrowly by the courts in order to limit the level of infringement which it makes on the right to freedom of expression. In the case of *Director of Public Prosecutions v McConnell*[6] the court held that it was for the court to determine as a question of fact whether or not a message was 'grossly offensive' by applying the standards of an open and just society, taking into account the context of the words and all relevant circumstances. There is furthermore an intent requirement on the part of the sender. In this case, a Christian pastor had made negative remarks on Islam during a sermon which was later streamed on the internet. The court, taking into consideration the accused's right to freedom of expression as protected under the ECHR held that his expression was merely offensive. The court also reiterated that courts must be careful not to allow the criminal law to censor speech which is merely offensive.[7] In an earlier case, the House of Lords had held that the offense in Section 127 of the Communications Act went no further than necessary in restricting the right to freedom of expression.[8] The section has the legitimate aim of protecting the rights and reputations of others from attack through the use of the public electronic communications network without making unnecessary inroads into the rights of the communicator.

Indeed the UK's Crown Prosecution Service has gone ahead and issued guidance to prosecutors on how to handle cases arising out of computer misuse, including those involving offensive communication. The Guidelines first note that cases may be more appropriately prosecuted under other laws. Prosecutors are expressly required to balance between the right to freedom of expression and the public interest. The context within which the communication as made must also be considered and the provisions of article 10 of the European Charter on Human Rights. The prosecution must both be necessary and proportionate to what was done.[9]

The UK's offensive communication provisions sets a good example for Uganda and other countries in that only grossly offensive communications are

4 As amended by S.43 (1) of The Criminal Justice and Police Act 2001

5 See Art 10 of the European Convention on Human Rights.

6 [2016] NIMag 1.

7 F Cranmer '"Grossly offensive" or merely "offensive"? *DPP v McConnell:* A note' *Law and Religion UK* 5 January 2016.

8 *Director of Public Prosecutions v Collins* [2006] UKHL 40.

9 The Crown Prosecution Service 'Guidelines on prosecuting cases involving communications sent via social media' available online at http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/ (accessed 15 October 2017).

criminalised and that there has to be intent to insult on the part of the sender. The provisions, and the way they have been applied by the courts, strikes a balance between protection of the right to dignity and the right to freedom of expression. Such provisions cannot easily be used for ulterior purposes such as clamping down on vulnerable minorities and quieting political dissent.

India

India has recently taken a bold step toward the protection of the freedom of expression by declaring unconstitutional its offensive communication provision. Offensive communication was provided for in the Information Technology Act 2000. Section 66 A thereof makes it an offense to send information that is grossly offensive or of a menacing character or to send any information which the sender knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will by making use of a computer resource or a communication device. The section further criminalised sending an electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or mislead the recipient about the origins of the message. The punishment imposed for this offense was imprisonment for up to three years with a fine.

This section was challenged in the Supreme Court in the case of *Shreya Singhal v Union of India*.[10] The Court considered the provision in light of Article 19 of India's Constitution, which guarantees the right to freedom of expression. Article 19(2) provides that the freedom of speech and expression may be restricted by a law where this serves 'the sovereignty and integrity of India, the security of the State, friendly relations with other States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence.' The Court held that Section 66A was unconstitutional on the basis that it was over-broad and vague. The Act failed to define and delineate clearly the instances in which the Act would apply.

Tanzania

Tanzania has recently adopted the Cybercrimes Act, 2015 to make provision for the criminalisation of offences related to computer systems and Information Communication Technologies. The Act has two provisions that are comparable to the 'offensive communication' provisions in the legislation of Uganda, the United Kingdom and India. Section 18 of the Act prohibits insults through a computer system on the basis of race, colour, descent, ethnicity, nationality or religion. The offence is punishable with a fine or imprisonment of not less than one year. This provision delineates more clearly the kind of communication that is prohibited than the Ugandan legislation which merely states that 'offensive' communication is prohibited. It also makes a point to criminalise communications which have the potential to have serious harmful consequences to nation building as opposed to communications which are merely 'offensive'.

The Ugandan Act could perhaps be amended to deal with specific, defined offensive communications, transmitted through a computer system, which are known to be likely to feed into volatile situations such as tribal conflict. Uganda may draw a lesson from its neighbor in avoiding the use of criminal law to regulate and address the communication of expressions which are merely offensive to individuals.

Conclusion

Along with technological advancement, there is a continuous need for legislation which keeps up with evolving means of committing crimes. The four jurisdictions considered have each dealt differently with communications transmitted through computer systems and which are offensive to the recipient. A fine line has to be drawn between the regulation of offensive communication through the use of computers and unwarranted limitation of the right to freedom of expression. The UK puts in place enough safeguards so that the right to freedom of expression is protected while also protecting persons from very offensive communication. India on the other hand has it offensive communications law struck down for being unconstitutional, while Tanzania does not use vague and broad language but clearly defines what it criminalises. Thus of the three countries at the different levels of development that have been discussed here, Uganda stands alone in maintaining such a vague provision. Section 25 of Uganda's Computer Misuse Act, 2011 is undoubtedly susceptible to constitutional challenge due to its broad and vague nature and would benefit from an amendment which either limits criminalisation to 'grossly offensive' communications or delineates the offence to only apply to communications which are likely to incite violence and hatred through the use of a computer system. The decision of the Constitutional Court in the case of Andrew Karamagi & Robert Shaka is thus eagerly awaited.

10 See Writ Petition No.167 Of 2012.

INTERNATIONAL LAW PERSPECTIVE

How does the Computer Misuse Act measure up to international standards of privacy and freedom of expression on the Internet?

Linette du Toit
Researcher, HRAPF

Introduction

This article analyses the Computer Misuse Act, 2011 from an international law perspective. It focuses on the internet, a key aspect of computer communications. It analyses the compatibility of the Act with international human rights standards on privacy and freedom of expression on the internet. In the first part of the article, the applicable principles provided under international law will be set out and discussed. In the second part, selected provisions of the Act will be analysed and considered in light of the stated recognised principles in order to determine their level of compatibility with international human rights law. The purpose of the Act is 'to make provision for the safety and security of electronic transactions and information systems', 'to prevent unlawful access, abuse or misuse of information systems including computers' and 'to make provision for securing the conduct of electronic transactions'.[1] It is expected that the objectives of securing information systems and preventing the misuse of information should be carefully balanced against the rights to privacy and the right to freedom of expression.

1. The international legal framework on the right to privacy and freedom of expression on the internet

The rights applicable generally also apply to the internet. Therefore, the international legal framework on the right to privacy and freedom of expression applies to the internet too.

a) The right to privacy

The right to privacy is protected under Article 17 of the International Covenant on Civil and Political Rights (ICCPR)[2]:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

The right is also protected under Article 12 of the Universal Declaration of Human Rights:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

This right is furthermore protected in the United Nations Convention on Migrant Workers[3] and the United Nations Convention on the Protection of the Child.[4]

The United Nations Human Rights Committee, in interpreting Article 17 of the ICCPR, has stated that any interference with privacy have to be envisaged by law and that the law on which such an interference is based has to comply with 'the provision, aims and objectives of the Covenant', otherwise the interference will nevertheless be unlawful.[5] The Committee has expressed that even an interference provided for under the law can be classified as an 'arbitrary interference' if it is not reasonable to interfere with the privacy of the individual in the particular circumstances of the case.[6] The Committee recognises that

1 According to the long title of the Act.

2 Adopted by the General Assembly of the United Nations in 1966 and ratified by Uganda in 1995.

3 Art 14.

4 Art 16.

5 Human Rights Committee General Comment No. 16, U.N. Doc CCPR/C/CG/16 (8 April 1988) (Article 17: Right to Privacy: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) at para 3.

6 n 5 above at para 4.

competent public authorities should be able to access information relating to the private lives of individuals if such knowledge is essential for the protection of the 'interests of society' as protected under the Covenant.[7] Interference in private life needs to be governed by law and needs to specify in detail the exact circumstances under which interferences would be permitted.[8]

State parties are under a duty to provide a legal framework prohibiting interferences inconsistent with the ICCPR.[9] Importantly, the Committee states that the gathering and holding of personal information on computers and other devices must be regulated by law and that States have to take effective measures to ensure that information concerning a person's private life does not reach the hands of an unauthorised person.[10]

b) The right to freedom of expression on the internet

The right to freedom of expression is protected under the ICCPR as well as the Universal Declaration. Article 19 of the ICCPR provides:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (ordre public), or of public health or morals'

Article 19 of the Universal Declaration provides:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The United Nations Human Rights Committee, the body that oversees the ICCPR, has stated that the right to freedom of expression includes electronic and internet-based modes of expression.[11] Article 19(2) explicitly extends beyond the content and also cover the means of communication.[12] It includes 'any other media', which is interpreted to extend to the internet.[13]

The Human Rights Committee has also made it clear that in order for a norm to be characterised as 'law', it is essential for the provision to have been expressed with the necessary precision that would enable members of the public to adapt their conduct accordingly.[14] Laws must also provide sufficient guidance to those responsible for their enforcement in order to know with certainty which conduct is restricted.[15]

In 2011, representatives of three regions - Africa, the Americas and Europe[16], as well as the UN Special Rapporteur on Freedom of Expression and leading international Non-Governmental Organisations advocating for freedom of expression[17] agreed on the international law principles concerning the internet and freedom of expression. The Joint Declaration on Freedom of Expression and the Internet (JDFEI) was subsequently adopted. The Declaration summarises the international

7 n 5 above at para 7.

8 n 5 above at paras 7-8.

9 n 5 above at para 9.

10 n 5 above at para 10.

11 Human Rights Committee General Comment No. 34, U.N. Doc. CCPR/C/GC/34 (12 September 2011) (describing the application of art. 19 of the ICCPR on freedoms of opinion and expression).

12 See M Land 'Toward an International Law on the Internet' (2013) 54 *Harvard International Law Journal* 401.

13 As above.

14 As above.

15 As above.

16 These representatives were the African Commission on Human and Peoples' Rights' Special Rapporteur on Freedom of Expression; the Special Rapporteur for Freedom of Expression of the Inter-American Commission for Human Rights of the Organization of American States and the Organisation for Security and Cooperation in Europe Representative on Freedom of the Media.

17 ARTICLE 19, Global Campaign for Free Expression and The Centre for Law and Democracy.

law principles pertaining to the exercise of the freedom of expression in an online context and will therefore be used as the standard for considering the compatibility of the Computer Misuse Act, 2011 with the international law standards in respect of this right.

The principles stress that the internet has a transformative nature which enhances the ability of billions of people to express themselves and to access information. They also acknowledge that some governments have taken action which unduly restricts the freedom of expression on the Internet and which fails to take into consideration the particular characteristics of the Internet, resulting in an undue restriction of the right to freedom of expression.

The JDFEI covers the following six aspects:

i) General principles
The Declaration makes it clear that restrictions on freedom of expression on the internet are only acceptable if they are provided for by law which is clear and accessible and is necessary to protect an interest recognised under international law. According to the ICCPR, such 'interests' recognised under international law include the respect of the reputation and rights of others and the protection of public health and morals, national security or public order.[18] The principles state that the interest that a restriction is protecting must be weighed against its impact 'on the ability of the internet to deliver positive freedom of expression outcomes'.[19] The principles suggest self-regulation as a tool for addressing harmful speech and promote internet literacy.[20]

ii) Intermediary liability
Providers of technical internet services should not be held accountable for the content generated and transmitted, unless they had intervened in the content or have failed to carry out a court order requiring them to remove the content.

iii) Filtering and blocking
The blocking of entire websites and types of uses – such as social networking – is an extreme measure which can only be justified in accordance with international standards.

iv) Criminal and civil liability
The principles suggest that legal cases relating to internet content should be undertaken in the States to which the cases have a real and substantial connection. Private parties should bring cases in a jurisdiction where they can establish they have suffered substantial harm. Standards of liability should consider the overall public interest in protecting both the expression and the forum in which it is made.

v) Network neutrality
This aspect of the principles provide that there should be no discrimination in the treatment of internet data and traffic, based on factors such as the author or the origin and destination of the content. Internet intermediaries should furthermore be required to be transparent in respect of their information management practices.

vi) Access to the internet
According to this aspect of the principles, States are obliged to promote universal access to internet in order to give effect to the right to freedom of expression. It is recognised that access to internet is necessary in order to promote respect for other rights and that cutting off access to the internet can never be justified. To deny individuals access to internet as a form of punishment is also an extreme measure. Other limitations, such as requiring providers to register, have to comply with international standards in order to be legitimate.

2. Compatibility of the Computer Misuse Act, 2011 with international human rights standards

In this section, selected provisions of the Act will be discussed in terms of compliance with the international human rights standards set out above.

a) The right to privacy
The Act fails to meet the international standards in respect of the right to privacy in various ways.

Firstly, Section 9 of the Act allows an investigative officer to obtain an order for the preservation of data, stored or processed by means of a computer system or other information and communication technologies. The only grounds detailed to justify such an order being granted is that there should be 'reasonable grounds' to believe that data is 'vulnerable to loss or modification'. Contrary to the requirements of the international law regime, the law does not specify in detail the precise circumstances under which an interference in the

18 Art 19(3).

19 General Principle 1(b).

20 General Principle 1(e).

right to privacy will be permitted.[21]

Section 9(3) of the Act suggests that the purpose of the preservation order would be to retain data which could serve as evidence in the case of suspected criminal activity. The Act, however, omits providing details on the seriousness of the crimes involved and the importance of the evidence, held on a computerised system, for the prosecution of the crime. As it stands, suspicion of *any* offence would fall within the ambit of the section. The officer would need to meet a very low standard of proof in justifying the granting of the preservation order. Even though international law requires that private information of individuals ought to only be accessed where this is essential for the protection of the interests of society (as recognised under the ICCPR), this provision provides for such an infringement on the mere suspicion that an offence of negligible gravity had been committed.[22] The Act is furthermore unclear in as far as the meaning of 'retention of data' is concerned. The Act does not set out whether the order is against the owner or controller of the data to prevent them from destroying or modifying the data or whether it gives someone else the right to preserve the data. It is also not made clear whether the Act intends for the relevant data to be taken off the device or whether the whole device ought to be retained. The Act furthermore fails to create safeguards for ensuring that the private data is accessed in the process of taking the relevant data off the device.

The Act, however, omits providing details on the seriousness of the crimes involved and the importance of the evidence, held on a computerised system, for the prosecution of the crime.

21 n 5 above at para 7-8.

22 Unwanted Witness & Civil Rights Defenders 'Analyzed Cyber Laws of Uganda 2016' (2016).

Along the same vein, the Act in Section 10 provides that an investigative officer may apply to a court of law for an order for the disclosure of all preserved data and the path through which the data was submitted. Section 11 of the Act provides that an investigating officer may apply to court for an order compelling any person to submit specified data in that person's possession or control, which is stored in a computer system and any services provider to submit subscriber information in its possession or control. Once again, the Act does not require any prima facie evidence on the part of the investigating officer in order to justify the granting of such an order.

The Act does not provide for the interference with the right to privacy to be weighed up against the interests which such an interference aims to achieve and falls short of 'the provisions, aims and objectives of the Covenant' in that regard.[23] The interference with privacy detailed in section 9 to 11 of the Act can therefore be regarded as unlawful under international law standards.

In Section 28 of the Act, police officers are given broad powers of search and seizure where they suspect that an offence has been committed under the Act. A Magistrate may grant an order to enter and search premises if the police officer can provide reasonable grounds for believing that an offence has been committed or is about to be committed under the Act. An authorised officer is furthermore permitted to seize computer systems or take samples or copies of applications or data which are believed to have been used or is intended for use in the commission of an offence. 'Reasonable grounds' does not require a high level of evidence for the granting of an extremely invasive order. Considering the vagueness of many of the offences provided for in the Act, as will be discussed in greater detail below, this section seems to make provision for the granting of invasive orders on flimsy grounds.

b) The right to freedom of expression

As discussed elsewhere in this issue, there are a number of provisions in the Act that create offences, punishable with imprisonment, but are not clearly and unambiguously defined. These offences appear in Section 24 and Section 25 of the Act and criminalise 'Cyber harassment' and 'Offensive communications' respectively. Apart from the constitutional standard for the limitation of the right to freedom of expression which these offences fail to meet, they also represent violations of the right in terms of international law

23 n 5 above at para 4.

standards.

Firstly, the ICCPR makes is clear that it is only 'arbitrary' and 'unlawful' interferences with a person's privacy that are prohibited.[24] The right to freedom of expression may be limited by a 'law'.[25] The Human Rights Committee has expressed that a norm can only be characterised as 'law' if it is expressed with the necessary precision that would inform members of the public about exactly which conduct is prohibited.[26] Under the crime of 'Cyber harassment', the terms 'obscene, lewd, lascivious or indecent' are not defined, yet requests or proposals qualifying as such are regarded as offences punishable by law. Equally, under the offence of 'Offensive communications', the term 'breach of peace' is not defined and can be taken to apply to a very broad range of actions. The undefined offences create uncertainty

Secondly, international law provides that laws must also provide sufficient guidance to those responsible for their enforcement in order to know with certainty which conduct is restricted.[27] In the same way that the undefined terms in the offences create uncertainty to those to which the law applies, it also grants unguided discretion to the implementers of the law. Enforcement officers can only rely on their subjective understanding of the offence and may easily be swayed by their personal prejudices and preconceived ideas in applying the law.

Finally, contrary to the principle of 'Network neutrality' as agreed to under the JDFEI, Section 24 and 25 have been applied to target particular individuals.[28] This principle provides that there should be no discrimination in the treatment of internet data and traffic, based on factors such as the author of the content.[29] Charges have rarely been laid under these provisions apart from in cases where the author of the content are known critics of the leadership of the country.[30] It is clear that these provisions are not in line with the safeguards imposed and expected by international human right law and that the right to freedom of expression is arbitrarily infringed by this Act.

3. Conclusion

The Computer Misuse Act misses the mark as far as international standards of privacy and freedom of expression are concerned. International human rights law recognises the infringement of rights which the Act facilitates and its failure to give expression to the rights as required by the various treaties. The Act is in need of urgent amendment in order for Uganda to comply with its obligations, freely taken on as a member of the international community.

SOURCE: https://www.shutterstock.com

24 Art 19(1) of the ICCPR.

25 Art

26 As above.

27 As above.

28 See discussion above under 'Freedom of Expression'.

29 As above.

30 Notably, two of the persons to have been charged under these provisions are two well-known critics of the Museveni regime: Stella Nyanzi and Robert Shaka. See details of these cases in case updates below.

COMMENTARY

Provisions of the Computer Misuse Act and how they violate constitutionally protected rights of LGBTI persons in Uganda

Patricia Kimera
Head, Access to Justice Division, HRAPF

Introduction

Even though there have been improvements in the treatment of LGBTI people across some parts of the world as well as legal recognition of their basic humanity, dignity and fundamental rights and freedoms, it remains a fact that a number of countries in the world, Uganda being one of these, are still quite hostile toward LGBTI people. In 2011, the government enacted the Computer Misuse Act, 2011 for the preservation and protection of computer data and programs from unlawful interference and access, as well as protecting private individuals from interference with their privacy and attacks on their character through offensive communications, cyber stalking and harassment and unauthorised access to and modification of computer data and programs. The basic idea was to protect the privacy of individuals, to preserve data for purposes of law enforcement and to protect vital data from wanton distraction. Unfortunately, this Act is likely to be problematic for LGBTI persons because it has some sections which, if interpreted and enforced against Uganda's homophobic, transphobic, and biphobic background, will have catastrophic effects for the constitutionally protected rights of LGBTI persons in Uganda. Some of these sections are inherently harmful whereas others merely have the potential to be harmful given the context in which they are likely to be enforced. This article considers the likely implications of some provisions of this Act for the rights of sexual minorities in Uganda, and also the real implications as already recorded by HRAPF.

The Constitution of Uganda and the rights of LGBTI persons

The Constitution of the Republic of Uganda is the supreme law of the country to which any other law must conform and derive its validity[1] and any other law that is inconsistent to it is void to the extent of its inconsistency. Despite the absence of a specific provision in the Constitution that expressly recognises rights of LGBTI persons, the High Court and the Constitutional Court in Uganda have affirmed the universality of Human Rights as entitlements to every one irrespective of their sexual orientation and gender identity and perceptions of the majority of the populace. These pronouncements have been made in various cases as discussed below.

Victor Juliet Mukasa and Yvonne Oyo v AG[2]**:** The case involved the unlawful interference with the applicants' privacy through unauthorised search. The unlawful search was conducted by the police and local authorities on suspicions that the applicants were homosexuals. The search was allegedly intended to unearth evidence of homosexuality. In the process, one of the applicants was arrested, fondled and denied access to toilets by the police officers. Upon hearing the case, the High Court found that the actions amounted to breach of fundamental human rights and were a violation of various human rights instruments. It was emphasised that it did not matter that the applicants were actual or suspected homosexuals. The ruling was a landmark in clarifying the principle of universality of human rights that accrue to all irrespective of their sexual orientation or Gender Identity and as a bar to arbitrary police intrusion into the private lives of persons.

Kasha Jacqueline and 3 others v Rolling Stone Newspaper[3]: In this case, the respondent tabloid

1 Art 2 of the Constitution of the Republic of Uganda, 1995 as amended.

2 Miscellaneous Application No. 24 of 2006.

3 Miscellaneous Application No. 163 of 2010.

published the photos, names and addresses of suspected homosexuals including the applicants, calling upon the public to hang them, as they were after children (allegedly recruiting children into homosexuality). In court, the applicants argued that their rights to privacy and dignity were violated, and the respondents contended that that was not the case as the applicants were openly homosexual. The judge clarified that the case was not about homosexuality but about fundamental rights and freedoms. The court further held that the scope of Section 145[4] was narrower than gayism generally and that one had to commit an act prohibited under Section 145 in order to be regarded criminal. The court therefore agreed with the applicants that there was a violation of rights.

The case of ***Jjuuko Adrian v AG***[5] challenged the constitutionality of section 15(6)(d) of the Equal Opportunities Commission Act, which barred the Commission from handling and investigating matters which are considered immoral and socially harmful and unacceptable by the majority of the cultural and social communities in Uganda. The Constitutional Court struck down the section as being unconstitutional for seeking to create a class of social misfits undeserving of the protection of the law in violation of Article 21. The import of the judgment is that every person in Uganda is deserving of protection of the law, and no-one should be discriminated against or suffer prejudice on grounds of morality or public opinion.

The above cases directly and indirectly fortify the position that LGBTI persons are entitled to the same rights as everyone else. It should however be noted that enjoyment of the rights provided for under the Constitution can be limited within the bounds of Article 43. This limitation should however not be beyond what is acceptable and demonstrably justifiable in a free and democratic society.[6] As far as LGBTI persons are concerned, same sex conduct is criminalised in the Penal Code Act and this was interpreted as a limiting factor on the enjoyment of their rights in the case of *Kasha J. Nabagesera and 3 Others v AG and Rev. Fr. Simon Lokodo*,[7] in which the High Court acknowledged the applicants' rights to associate, express and assemble, but noted that this was limited by the Penal Code's criminalisation of same sex conduct. The case is however subject of an appeal.

4 Penal Code Act Cap 120.

5 Constitutional Petition No. 1 of 2009.

6 Art 43(2)(c).

7 Miscellaneous Cause No. 33 of 2012.

In conclusion, although the majority of the population in Uganda does not recognise LGBTI persons as entitled to the same rights as everyone else, the legal regime is protective of their rights and offers various mechanisms for their enforcement. Beyond Uganda's legal framework, the sub-regional, regional and international frameworks are also extensively protective and cognisant of the rights of LGBTI persons and have taken deliberate steps to enforce them.[8]

Key Rights that are violated/threatened by provisions of the Computer Misuse Act

i) The right to privacy

The right to privacy is guaranteed by Article 27 of Uganda's Constitution[9] as well as other international human rights instruments[10]. The Article prohibits unlawful search of a person, their property or home; and also prohibits unlawful entry by others on the premises of another person. This right underpins human dignity and other key values such as freedom of association and freedom of speech, and has become one of the most important issues in the modern age of technological advancement.

> **"The violation of this right [to privacy] is often rooted in simple curiosity by law enforcement officers and the general public but they are perpetrated in such a way as to give the process a cloak of legitimacy, thereby allowing egregious abuses of this right.**

In relation to LGBTI persons, privacy of body, home and correspondence is crucial to them particularly those who identify as transgender. The violation

8 Human Rights Awareness and Promotion Forum *A Guide to the Normative Legal Framework on the Human Rights of LGBTI Persons in Uganda* (2015).

9 Constitution of the Republic of Uganda, 1995.

10 See Art 12 of the UDHR, Art 17 of the ICCPR and General Comment No 16 on the right to privacy.

of this right is often rooted in simple curiosity by law enforcement officers and the general public but they are perpetrated in such a way as to give the process a cloak of legitimacy, thereby allowing egregious abuses of this right. Some of the more common violations of the right to privacy faced by LGBTI people in Uganda include unlawful/ unnecessary body searches, being forced to undress in order to ascertain one's gender/sex, being spied on by neighbours upon suspicion of one's sexual orientation or gender identity as well as invasions of their homes and offices to search through their properties and correspondences for evidence of unnatural offences upon suspicion of their sexual orientation and gender identity.[11]

The Computer Misuse Act provides in Part II for orders of court to preserve any data, disclose such data or produce it for purposes of investigating an offence, and this order can be obtained without the knowledge of the data subject since there is no requirement in the law that the subject be notified of such an order or application for it. Although sexual orientation and gender identity are not actually criminalised in Uganda with the law focusing on sexual acts, the ruse of 'investigating unnatural offences' is often used to harass, intimidate and dehumanise suspected LGBTI persons by both state and non-state actors.[12] This mode of enforcement has been transferred to the enforcement of the Computer Misuse Act, and was witnessed in a case where a transgender woman was charged under Section 24 of the Act[13] and the investigating officer admitted to having checked her Facebook account and found some 'strange pictures of her wearing dresses that instigated him to further probe about her gender identity'. Although the charges were later dropped, her right to privacy had been violated. This was done without obtaining the requisite court order. Even then, the order can easily be obtained as there is not much to prove besides 'reasonable suspicion' and the other party is not given a chance to oppose the application.

This is the same mischief likely to be occasioned by Section 28 of the Act which authorises a magistrate, upon an application by an investigating officer, to order the search of any premises and the seizure of any data, program, copies of data or any computers 'reasonably believed' to be evidence of the commission of an offence under the Act. This provision in much the same way as the foregoing provisions will impact negatively on the right to privacy of LGBTI persons in Uganda as it may be used injudiciously by law enforcement agencies to target them for the simple fact that they are an unpopular minority.

ii) The right to freedom of conscience, expression and belief

This right is protected under Article 29 of the Constitution of Uganda and in various international legal instruments which Uganda has ratified.[14] It is a right that has continually come under threat in Uganda of recent, with various persons who have expressed strong opinions criticising the government coming under scrutiny and even being dragged to court by the government in an attempt to curtail this freedom.[15] This Act now goes further to criminalise some forms of expression in Section 24 of the Act, which criminalises cyber harassment. Part of this section defines cyber harassment to include, among others, 'making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent.' As always with laws alluding to decency, morality or public dignity and interest, these concepts remain nebulous and ambiguous, giving wide discretion to the enforcing officer to determine what communication may qualify as 'lewd' or 'lascivious' or 'indecent'. This will expose suspected LGBTI persons to possible abuse when communications such as texts and emails between lovers are interpreted by law enforcers, because of the fact that such communications are between two persons of the same sex, to be indecent or lewd. The same criteria would of course not automatically apply to heterosexual couples in the same situation, unless there is a reason to target that person specifically.

11 See Human Rights Awareness and Promotion Forum and the Consortium on Monitoring Violations Based on Sexual Orientation, Sex Determination and Gender Identity *Uganda Report of Violations Based on Sexual Orientation and Gender Identity* (2015).

12 Refer to the Civil Society Coalition on Human Rights and Constitutional Law (SCCHRCL) and Human Rights Awareness and Promotion Forum (HRAPF) *Protecting morals by dehumanizing LGBTI persons? A critique of the enforcement of the laws criminalising same sex conduct in Uganda* (2013).

13 HRAPF/T/27/02/2017.

14 Art 9 of the African Charter on Human and Peoples' Rights; Art 18 of the International Covenant on Civil and Political Rights.

15 *Obbo and Another v Attorney-General* **Supreme Court of Uganda, Constitutional Appeal No. 002 of 2002** at paragraph 62**;** See also N Slawson 'Fury over arrest of academic who called Uganda's president a pair of buttocks' *The Guardian* 13 April 2017 available online at https://www.theguardian.com/global-development/2017/apr/13/stella-nyanzi-fury-arrest-uganda-president-a-pair-of-buttocks-yoweri-museveni-cyber-harassment about the arrest of Dr. Stella Nyanzi.

iii) The right to equality and freedom from discrimination

This right is provided for under Article 21 of the Constitution and provides that all persons are equal before and under the law and that a person shall not be discriminated against on grounds stipulated under Article 21(3). Although sexual orientation and gender identity are not protected grounds under the Constitution, Uganda is a signatory to the International Covenant on Civil and Political Rights (ICCPR). The Human Rights Committee,[16] which oversees this instrument, has declared sex as a protected ground, by implication binding Uganda which is a state party. In addition, as discussed above, all rights in the Constitution apply to persons equally, including LGBTI persons.

Given the homophobic nature of the enforcement of the various laws that affect LGBTI persons, it is quite plausible that this Act will result in the infringement of the right to equality of sexual minorities in Uganda in as far as there is great potential to use it to target unpopular minority groups.[17] These acts of unfair discrimination on the basis of sexual orientation or gender identity are given a kind of legitimacy on the grounds that same-sex sexual activity is prohibited in Uganda. In one of the cases handled at the legal aid clinic[18] a client was terminated from employment after being charged with the offence of cyber stalking which charges were later dismissed for want of prosecution. The charges were based on text messages that the person sent to a fellow woman, seeking a romantic relationship. It is arguably correct that if a person was sending the same text messages to someone of the opposite sex, these charges would not suffice. It is therefore plausible that sections of the Computer Misuse Act will be used to witch hunt persons of the same sex who innocently exchange sexual/romantic communications with others, merely on grounds that same sex expression of love is frowned upon.

iv) The right to a fair trial

This right is protected under Article 28 of the Constitution. Article 28(12) of the Constitution requires that every criminal offence be stated in clear and unambiguous terms for it to be an offence valid under the law. Vague and broadly defined offences are not constitutional despite their presence on the books of law and every arrest under such a law is a violation of the right to liberty. The Computer Misuse Act has various provisions that are broad and vague and would not pass the constitutionality test. Sections 24 and 25 of the Act that create the offences of cyber harassment and offensive communication respectively create broad undefined offences. These sections broadly prohibit 'indecent' 'lewd' and 'lascivious' conduct, and prohibit communication that 'attempts to disturb the peace' of another person, among others. These terms are not defined and it becomes hard to know what conduct exactly is criminalised.

> **...despite their [offences] presence on the books of law and every arrest under such a law is a violation of the right to liberty.**

Considering the prejudice faced by LGBTI persons in Uganda, these provisions are fertile ground for abuse, as has been seen in the above case where a woman sending text messages to another was considered a criminal offence under the Act. As was seen in that case, there was no evidence adduced by the state and it was dismissed for want of prosecution.

Conclusion

The LGBTI movement in Uganda has fought for and continues to fight for legal recognition of the rights and dignity of LGBTI persons on the same footing as all other persons. The Computer Misuse Act with its vague provisions can be abused if there are no safeguards for the respect and protection of fundamental rights. Whereas the government is allowed to limit the enjoyment of rights and freedoms, these limitations must be narrowly defined and must conform to the international standards to which Uganda has agreed. The Computer Misuse Act falls short of these accepted standards. As always, we still have great need to focus on advocacy for legal reform to do away with all legal provisions, particularly those that impose criminal sanctions, that are over-broad or vague and that can therefore be used to target LGBTI persons and legitimise homophobia and transphobia in Uganda.

16 *Toonen v Australia Communication* 488/1992, UN Doc CCPR/C/50/D/488/1992(1994).

17 See Human Rights Awareness and Promotion Forum *The Implications of the Enforcement of Idle and Disorderly Laws on the Human Rights of Marginalised Groups in Uganda* (2016).

18 NAK-C 200/2015.

OPINION

For Ugandan communicators in the wake of Dr. Nyanzi's arrest: how free is our freedom of expression?*

Arinda Daphine
Story teller, Lawyer and Poet

In March 2017 Stella Nyanzi; a 'thinker, scholar, poetess, lyricist, writer, Facebooker and creative producer'[1] was charged by the Uganda Police, for *offensive communication* contrary to section 25 of the Computer Misuse Act 2011.

The particulars of the offense read as follows:

> 'Stella Nyanzi … made a suggestion or proposal referring his Excellency Yoweri Kaguta Museveni as among others 'A pair of Buttocks' which suggestion/proposal is obscene or indecent.'[2]

Since Nyanzi's arrest, Ugandan communicators including those who utilize social media platforms such as Blogs, Facebook and Twitter have been debating the question, 'How *free* is our freedom of expression and when does offensive language become criminal?' This article seeks to contribute to that debate.

The freedom of expression is guaranteed under Article 29(1)(a) of the 1995 Constitution of the Republic of Uganda. This provision states that 'every person shall have the right to freedom of speech and expression which shall include freedom of the press and other media.' 'Other media' in this context includes social media platforms like Facebook that Stella Nyanzi utilized to voice her critique on how Uganda is being governed.

While the current Constitution is lauded for being progressive and democratic[3], it gives no definition of the right to freedom of expression. The old 1962 and 1967 Constitutions defined the right to freedom of expression as 'Freedom to hold opinion and to receive and impart ideas and information without interference.' This definition is still relevant today as was held by the Supreme Court of Uganda.[4]

Every person therefore has a right to hold an opinion as well as the right to decide whether to express it or not. An opinion can be disseminated through political discourse, canvassing, cultural and artistic expression, religious discourse, teaching, and through commercial advertising.[5] Stella Nyanzi

* An earlier version of this article was first published on Arinda Daphine's blog 'EVABella' on 20th April, 2017. It can be found at https://arindaphine.wordpress.com/2017/04/20/for-ugandan-communicators-in-the-wake-of-nyanzis-arrest-when-do-we-cross-the-line-of-freedom-of-expression/ (Accessed on 20th October, 2017).

1 Aljazeera and News Agencies, *Museveni critic Stella Nyanzi to Appear in Court*, 10th April, 2017, Available online http://www.aljazeera.com/news/2017/04/museveni-critic-stella-nyanzi-court-170410074726763.html (Accessed on 20th October, 2017).

2 Bwesigye Bwa Mwesigire, African Arguments, *Uganda: Stella Nyanzi Charged for Calling President Museveni a "Pair of Buttocks"*, April 10, 2017. Available online http://africanarguments.org/2017/04/10/uganda-stella-nyanzi-charged-calling-president-museveni-pair-buttocks/ (Accessed on 26th October, 2016).

3 JP Muto-Ono P 'Freedom of Expression "Uganda Laws Best in Africa"' *Black Star News* 23rd July 2015. Available online http://www.blackstarnews.com/global-politics/africa/freedom-of-expression-%E2%80%9Cuganda-laws-best-in-africa%E2%80%9D-media (Accessed 11 November 2017).

4 *Obbo and Another v Attorney General* 20040 AHRLR 256 9ugSc 2004 available online http://www.chr.up.ac.za/index.php/browse-by-subject/486-uganda-obbo-and-another-v-attorney-general-2004-ahrlr-256-ugsc-2004.html (Accessed 11 November 2017).

5 Human Rights Committee, General Comment No. 34, 12th September 2011. Available online http://www.refworld.org/docid/4ed34b562.html (Accessed 11 November 2017).

SOURCE: www.washingtonpost.com

Dr. Stella Nyanzi

prefers cultural and artistic expression. In 2016 she staged an undress protest at Makerere University and while her actions were misconstrued as lewd, she was making a strong cultural statement that resonates with what Aili Mari Tripps said:

> 'Women give life, and so to put the most private symbols of motherhood into the public arena is to negate that life, and say those in power are dead to Society'[6].

'Pair of Buttocks' is an artistic and cultural expression. Charles Onyango Obbo explains the connection between Nyanzi's words and culture when he writes,

> '... the derriere ... is also where we get rid of the waste in our bodies, and the most stinging source of African insult. Nyanzi drew from the latter.'[7]

The term 'offensive' should only be accorded to grave expressions such as those that incite discrimination on the basis of race, religion or nationality. In *Malcom Ross v Canada*,[8] a teacher lost his teaching position because of the expression of his views as an author. The Human Rights Committee stated that this was a restriction on his freedom of expression that had to be justified. It was held that the author's statements were discriminatory against persons of the Jewish faith and ancestry and therefore the restriction was justified on those grounds.

Besides Stella Nyanzi, other Ugandans have had their right to freedom of expression gagged on grounds of 'offensive language'.

Recent developments in Uganda reveal that most of what is referred to as 'offensive language' by the state is usually personal opinions against the

6 The real African *Undress for Redress: The Rise of Naked Protests in Africa* 15th June 2016.

7 C Onyango Obbo, *Uganda: 'A pair of Buttocks" and the Big Silent War Over the Museveni Years*. The Monitor 19th April , 2017. Available online http://allafrica.com/stories/201704190015.html (Accessed 11 November 2017).

8 *Malcom Ross v Canada* The Human Rights Committee, Communication No. 736/1997, UN DOC. Available online http://hrlibrary.umn.edu/undocs/736-1997.html (Accessed 11 November 2017).

regime and does not qualify to be categorised as 'offensive'.

Besides Stella Nyanzi, other Ugandans have had their right to freedom of expression gagged on grounds of 'offensive language'. In October 2016, the Uganda Communications Commissions (UCC) issued a directive against NTV compelling the TV station to stop broadcasting programmes featuring Frank Gashumba as a guest speaker because the political analyst was allegedly using profane and abusive language.[9] In November 2015, the UCC issued a similar directive against five radio stations as well as four television stations, which routinely hosted Mirundi Tamale, a renowned political analyst.[10]

The pertinent question to pose here is: in what circumstances is the state justified to restrict the right to freedom of expression?

The right to hold opinions and to impart ideas and information' is not an absolute one and according to Article 43 of the Constitution, it can be limited if its enjoyment will prejudice the freedoms of others or if public interest demands so. Ugandan communicators only cross the line of freedom of expression if their expressions threaten national security, or, public health, or, public order, or, public morals, or, amount to an infringement of the rights of others. Only then, can the State restrict the Communicator's freedom of expression. However before being imposed, the restriction must be subjected to the three tests:[11] it must for be provided by the law, have a legitimate aim and must be necessary.

Regarding the first test, the law that was relied on in the case of Stella Nyanzi is the Computer Misuse Act 2011 which creates the crime of 'offensive communication'. Section 25 of that law provides that a person commits the crime when he/she willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no legitimate purpose. Determining what amounts to 'disturbing the peace and quiet' is a legal question that must be answered before convicting the individual.

In 1985 Yong-Joo Kang of Korea was arrested and detained under allegations of contravening the National Security Law because he wrote publications that were said to be aimed at destroying the free and democratic basic order of Korea. The Human Rights Committee heard his case and found that any law that compels an individual to alter his/her political opinion restricts the freedom of expression.[12] Holding a dissenting view about the ruling party does not amount to 'disturbing the peace' and therefore Ugandan communicators are entitled by right to hold opposing opinions against the government and to express these opinions through various mediums.

Secondly, the restriction must have a legitimate aim. The law should be aimed at protecting national security, or, public health, or, public order, or, public morals, or, the rights of others. A desire to shield a government from criticism can never justify restrictions on free speech as was enunciated in the case of Yong-Joo Kang above.

Thirdly, the restriction must be necessary. In *Obbo and Another V Attorney General*[13], a case challenging the law criminalizing the 'publication of false news', the Supreme Court of Uganda expounded that this test has three elements; it requires that the objective of the restriction should be sufficiently important to override a fundamental right, that the measures set to achieve the objective must not be arbitrary, unfair or based on irrational considerations, and, that those measures must be proportionate and necessary to achieve the objective of the restriction.

Ugandan Communicators should boldly hold and express their views, plainly or metaphorically. We should not be intimidated when the State threatens us, as has been done to some of the vocal political analysts. If we know when the restrictions on our rights apply, then we can comfortably speak our minds. Criticism of government is pertinent in attaining a free and democratic Uganda and we can legally do this using our art, our words and our bodies as long as we keep within the permissible boundaries set by both national and international laws.

9 UCC Statement to NTV Uganda, 10th October 216. Available online https://www.scribd.com/document/329243268/UCC-statement-to-NTV-Uganda (Uploaded by African Centre for Media Excellence) (Accessed 11 November 2017).

10 N Bwire & N Wesonga, *UCC Blocks Mirundi from TV, Radio*, Daily Monitor, 2nd December, 2016. Available online https://www.scribd.com/document/329243268/UCC-statement-to-NTV-Uganda

11 Art 19(3) of the International Convenant on Civil and Political Rights.

12 *Yong-Joo Kang v Republic of Korea*, Communication Number 878/1999 U.N. Doc. Available online http://hrlibrary.umn.edu/undocs/878-1999.html (Accessed 11 November 2017).

13 Supra, note 4.

COMMENTARY

How the Computer Misuse Act, 2011 silences dissenting voices

Dorothy Mukasa
Research Officer,
Unwanted Witness

In 2011, the President of Uganda assented to the Computer Misuse Act, 2011. He thus added to the number of already existing cyber laws in the country. The legislation was introduced due to an increase in the number of citizens utilising the internet and thus the need to control the internet more. However, rather than introducing it for real protection reasons, the Act was introduced more as a way of controlling the internet, as the state saw it as one of the remaining independent platforms where a decent and sound debate can take place and where ideas can be shared without political interference.

As a result, the online space is increasingly shrinking as actions that threaten the enjoyment of online freedoms and rights in Uganda are stemming from the existing cyber legal framework, including the Computer Misuse Act, 2011. The Act is responsible for creating offences related to computers and introducing heavy penalties. The offences include: as cyber harassment, child pornography, offensive communications and cyber stalking. The maximum penalties for these offences range from 1 to 5 years of prison with the exception of child pornography, which generates a maximum sentence of 15 years.

In the framers' perspective, the Act makes provision for safety and security of electronic transactions and information systems, to prevent unlawful access, abuse or misuse of information systems including computers. This presents a rosy picture of the Act while its deeper analysis reveals the violation of citizens' rights to privacy, freedom of expression and access to information.

Indeed, the Act is commonly used by security agencies to criminalise freedom of expression online, particularly Section 25 of the Act, which has been repeatedly invoked to charge users with offensive communication. Notably, individuals charged had expressed dissenting political views. Individuals like former Makerere research fellow, Dr. Stella Nyanzi and political activists Swaibu Nsamba are among those that have faced the wrath of this section.

> **... the Act sets vague definitions for conditions required for the offences to be at hand thus contravening the requirement of both unambiguous and foreseeable provisions in International law and can have a hampering effect on freedom of expression.**

In describing liability for offences related to computers, the Act sets vague definitions for conditions required for the offences to be at hand thus contravening the requirement of both unambiguous and foreseeable provisions in International law and can have a hampering effect on freedom of expression. The Act also gives police officers wide discretionary powers to search and seize if they suspect commission of an offence and yet the level of evidence required is low, only amounting to the reasonable grounds in order for the extensive search powers to be triggered. These far reaching powers of search and seizure combined with the low threshold of evidence required constitute a threat to privacy and freedom of expression.

Notwithstanding, the awareness of these extensive powers can have a chilling effect on the use of freedom of expression in the digital environment as people can be afraid of risking a police search on loose grounds.

OPINION

Computer Misuse Act 2011: Rule of by law under pax Musevenica

Andrew Karamagi,
Lawyer and Political Activist

Argument

There is no humane way to rule people against their will.

'To protest in the name of morality against "excesses" or ''abuses'' is an error which hints at active complicity…" wrote Simon de Beauvoir.[1]

It is in the same spirit that I invite the reader to think about and interpret the Computer Misuse Act of 2011. It is one of a series of incessant excesses that have been visited onto civic space in Uganda by the Museveni Administration.

It is neither an aberration nor is it a mistake; it is a logical progression (or more accurately, a natural regression) of a hybrid regime that is increasingly intolerant of both alternative thought and dissent.

Substantive Article

In addition to coloured water cannons, stockpiles of teargas, batons and pepper spray to quell demonstrations and protests, a regime such as the one that Gen. Yoweri Museveni leads must naturally enact laws like the antiquated Political Parties and Organisations (Amendment) Act Number 2 of 2010, the infamous Public Order Management Act 2013, the dubious Anti-Money Laundering Act 2013, the annulled Anti-Homosexuality Act of 2014, the misogynist Anti-Pornography Act of 2014, the Non-Governmental Organisations Act 2016 and the latest amendments to the Anti-Terrorism (Amendment) Act of 2017.

Oppression is a sine qua non for regime longevity.

Put in other words, oppression must become legal. Suffice it to say that the legislative agenda of the long-standing Museveni Regime over the past decade has left a clear and unmistakable footprint that aspires to criminalise constitutionally-protected liberties and freedoms like assembly, association and expression.

This can be gleaned by a cursory perusal of the Hansard, as the foregoing litany of Acts shows. This is the backdrop against which the Computer Misuse Act of 2011 should be viewed and understood. It is not a stand-alone legislation but a natural evolution of a political establishment that brooks no dissent.

Far from the rosy wording of the Act's objective which purports to have been enacted to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment, Sections 9 through 11 of the law as a matter of fact aspire to enable state intelligence agencies to overstep privacy rights without restriction and proffer charges on the basis of an individual's refusal to so disclose 'data' which has been broadly, vaguely and disproportionately defined to mean and include electronic representations of any form. Under these three sections (9-11) any person can be compelled to hand over any 'data' for purposes of assisting with investigations. It doesn't matter if my tablet computer's memory card contains my private health information, bank statements or privileged communications: I must hand it over and trust(!) the state to behave prudently with my information as it

1 N Klein *Shock Doctrine: The Rise of Disaster Capitalism* (2008) 132.

pursues whatever investigation.

Telecom service providers are equally compellable.

Contrary to the tenets of criminal law which requires specificity, Section 12 creates indeterminate offences that are open to overly broad and arbitrary definitions given the unique and evolving nature of information and computing technologies.

Section 13 concerns itself with 'access with intent to commit or facilitate the commission of a further offence.' It is not clear how the State will lead evidence insofar as the intention of an accused person to commit or facilitate the commission of a further offence will be proved or disproved.

Section 14 worsens an already bad situation by (potentially) enacting to the effect that private information stored on a computer may not be concealed, protected or modified for whatever reason, notwithstanding that the user is the owner of the said device. The Section does not take into consideration the work of the broad range of artists whose work revolves around use of information to convey a particular message. This provision is equally ripe for abuse and misuse.

Section 18 and 20 are not accommodative of the place of whistleblowers who by their very nature engage in the disclosure of unauthorised information of the kind that is enumerated under sub-sections (2)(a) to (d).

The most egregious enactment under this law is arguably Sections 24 and 25 which create the crimes of cyber harassment and offensive communications respectively. As I have argued in a yet-to-be-heard petition that I filed with another citizen, Robert Shaka, before the Constitutional Court, I find the impugned Section to be an excessive restriction on my freedom of speech and expression.[2] It provides the Director of Public Prosecution unbridled administrative and prosecutorial discretion which has indeed resulted in several cases of selective prosecution of Internet users based on certain views deemed objectionable by the Government or high ranking politicians and public officers.

Two recent cases stand out: the arrest, detention without charge and later prosecution of my co-petitioner, Robert Shaka and my co-author,[3] Dr Stella Nyanzi. In the former case, the prosecution alleges that Shaka disguised himself as 'Tom Voltaire Okwalinga'—a popular anti-Establishment Facebook page—between 2011 and 2015, Kampala, of willfully and repeatedly using a computer with no purpose of legitimate communication, disturbed the right to privacy of President Museveni by posting statements regarding his health condition on social media.[4]

For her part, Nyanzi, who is an academic and critic of the Museveni Administration, was violently arrested, detained and slapped with a litany of charges, among them offensive communications, especially for referring to President Museveni as a 'pair of buttocks'.[5]

An erstwhile Police spokesperson, Fred Enanga, once circulated a warning about the dangers of making posting politically-related information or content on social media because of the likelihood of being prosecuted for the same. Indeed, a few people were interrogated by Police over such postings. This kind of behaviour and conduct by the Police is most reprehensible, amounts to an abuse of its civilian mandate and an affront to the Constitution.

Section 25 has placed journalists, artists, students and academics as well as the broader public in constant fear of violating the law.

2 *Andrew Karamagi & Robert Shaka v Attorney General*, Constitutional Petition No. 5 of 2016.

3 S Nyanzi & A Karamagi 'The socio-political dynamics of anti-homosexuality legislation in Uganda' 29:1 *Agenda* (2015) 24-38.

4 n 3 above.

5 S Allison 'Uganda: Stella Nyanzi, the vulgar activist, takes on the Pair-of-Buttocks-in-Chief' *Daily Maverick* 11th April 2017 available online at https://www.dailymaverick.co.za/article/2017-04-11-uganda-stella-nyanzi-the-vulgar-activist-takes-on-the-pair-of-buttocks-in-chief/#.WO8-AGz9Iy0 (Accessed 21 October 2017); N Slawson 'Fury over arrest of academic who called Uganda's president a pair of buttocks' *The Guardian* 13 April 2017 available online at https://www.theguardian.com/global-development/2017/apr/13/stella-nyanzi-fury-arrest-uganda-president-a-pair-of-buttocks-yoweri-museveni-cyber-harassment (Accessed 21 October 2017).

Section 25 has placed journalists, artists, students and academics as well as the broader public in constant fear of violating the law. This fear is obviously one of the intended consequences of the law. Without a doubt, this amounts to a violation of the right to free thought (and ultimately expression) which is the foundation of Article 29(1)(a) of the 1995 Constitution of the Republic of Uganda.

Needless to say, both Sections are also vague and overly broad. They fall short of giving proper notice of the conduct that they seek to proscribe and terms such as 'disturb or attempt to disturb the peace, quiet or right of privacy' are not defined in the Act, and cannot be conclusively defined by a regular user of the internet. Consequently, and consistent with the repressive agenda that is reflected by the laws preceding and coming after the Computer Misuse Act of 2011, the Police and governmental authorities will arrest and prosecute otherwise confused citizens in an arbitrary and whimsical manner.

Section 28 is, as with previously highlighted provisions, prone to abuse and selective application to the extent that it affords the State an unbridled ability to conduct searches and seizures on homes, office premises (especially media house), vehicles or crafts and any other location on the ostensible claim that there are reasonable grounds for believing that an offence under the Act has been or is about to be committed in any premises. This would embolden and provide 'legal' grounds for outrages like the police raid on The Monitor Publications in May 2013 which was executed on the flimsy grounds that a letter written (and already published) by the same newspaper, attributed to renegade Gen. David Sejusa was a threat to national security![6] What is to stop the regime from raiding, searching and seizing especially media houses on the pretext of the belief that an offence has or is about to be committed under the said Act?

Before the enactment of the Public Order Management Act in 2013, the Police routinely clobbered and dispersed peaceful demonstrations and protests arguing that they were illegal. This notwithstanding the Supreme Court decision to the effect that the Police had no power to prohibit public gatherings but only to regulate and provide security when such gatherings (about which the Police has been notified not requested to authorise) are so convened. The enactment of that law legalised what the Police was already doing but wanted to do with legal cover. The same can be said of the fortunately annulled Anti-Homosexuality Act of 2014 which afforded the regime the short-lived latitude to harass persons of sexual orientations that individual higher-ups within the regime find 'disgusting and unnatural'. The perennial harassment of Non-Governmental Organisations, particularly those involved in governance-related work, had to be codified in the NGO (Registration) Act of 2016 so that it continues under a veneer of legality. Similarly, the targeting of dissenting voices under the Anti-Money Laundering or Anti-Terrorism Acts had to be sanitised through the enactment of a law.

At the time of writing this piece, everybody is talking about the proposed amendment to Article 26 of the Constitution to allow for compulsory acquisition of land for public purposes—contrary to the current stipulation of the said Article which enacts to the effect that acquisition of private land by government must be done after prior and adequate compensation.[7] Yet several parcels of private (and in other cases public) land have been acquired without prior and adequate compensation. This has led to a phenomenon that is referred to as 'land grabbing'. It has occurred for years and is now commonplace—almost always perpetrated by those with possession or access to arms and/or 'political connections' that enable this criminality with absolute impunity. Amending Article 26 will in essence legalise land grabbing. Like the Public Order Management Act sought to criminalise the rights to assembly; the Anti-Homosexuality Act butchered equality before and under the law regardless of one's sexual orientation or other such distinction; the Computer Misuse Act was enacted for the sole purpose of proscribing dissent and contra-Establishment opinions as conveyed on social media sites and platforms.

It is a legislative agenda that is predicated on the unsustainable premises of subjugation and intimidation.

Yet, as history and current events continually remind us, a land ruled by fear can never be happy or secure.

6 S Kafeero 'Sejusa Letter: How we were closed, reopened' *Daily Monitor* 5th August 2017 available online at http://www.monitor.co.ug/News/National/Sejusa-letter-Monitor-Kayihura-Muhoozi-Grace-Akullo/688334-4044870-13my9qn/index.html (Accessed 21 October 2017).

7 Constitutional (Amendment) Bill No. 13 of 2017.

CASE UPDATE

#PairOfButtocks: Uganda v. Stella Nyanzi

Stella Nyanzi (PhD),
Makerere Institute of Social Research

Email:
snyanzi@misr.mak.ac.ug

Considering that I am the accused party in the most notorious local case based on the Computer Misuse Act (2011), it is a wonderful opportunity for me to provide an insight into Buganda Road Criminal Case No. 319 of 2017, *Uganda v. Stella Nyanzi*. I am writing in direct response to the intensity and volume of widespread local, regional and international interest in the case proceedings; arising from the lay public, legal practitioners, human rights advocates, academics, journalists and other public media workers, members of the opposition in Uganda, and social media users. Although several narratives have been told about this case, I value the opportunity to add my own interjection in which I tell my own story. However, it is noteworthy that in a bid to cancel my bail, the State Prosecutor has already alleged before court that my social media posts written subsequent to my release contravene the subjudice rule and are thereby in contempt of court. Thus, in this article, I will self-censor by desisting from discussing the merits and limitations of the arguments of the case. Rather, I will focus on providing the facts of the case, as well as detail the progress so far to the present time.

The Politics of Naming Cases

The charges leveled against me arise out of the Computer Misuse Act (2011). In a revised charge sheet from the headquarters of the Criminal Investigation Department dated 23rd March 2017, bearing reference number E/79/2017 and prepared by Deputy Assistant Superintendent of Police (D/ASP) Kayiza Henry, two counts of offences are stated – namely cyber harassment and offensive communication. These crimes respectively contravene sub-sections 24(1)(2)(a) and 25 of this legislation. The wording of this charge sheet, perhaps, heightened the notoriety of this case to its fever-pitch levels. Specifying the particulars of the first count of cyber harassment, the verbatim statement reads:

> Stella Nyanzi on the 28th January 2017 at Kampala district or thereabout used a computer to post on her Facebook page 'Stella Nyanzi' wherein she made a suggestion or proposal referring his Excellency Yoweri Kaguta Museveni as among others 'a pair of buttocks' which suggestion/ proposal is obscene or indecent.

The air waves, television screens, and newspapers comprising traditional public media and diverse social media platforms went into overdrive mode discussing the wording of 'a pair of buttocks'. Comedians, cartoonists, musicians, poets, dramatists and computer graphics designers produced creative works using this reference. Consequently #PairOfButtocks was organically created, circulated and trended for weeks on end on the World Wide Web – particularly on Twitter, Facebook and Instagram. Rather than arresting its further circulation, my arrest and pre-trial detention instead refueled the currency of this tongue-in-cheek metaphor that I applied to describe the president of Uganda. Copies of this charge sheet were shared widely on social media platforms – particularly Whatsapp, Facebook and Twitter.

On the charge sheet, the particulars of the second count - namely offensive communication – were stated verbatim as follows:

> Stella Nyanzi between January 2017 and March 2017 in Kampala district willfully and repeatedly used electronic communication to post messages offensive in nature via Facebook, transmitted over the internet to disturb or attempted to disturb the peace, quiet or right of privacy of His Excellency the President of Uganda Yoweri Kaguta Museveni with no purpose of legitimate communication.

On the night of 7th April 2017, I was abducted from a car by eight men and two women who

were not wearing uniforms. My immediate captor was wearing a woolen mask over his face. They neither had identification papers, nor an arrest warrant. They neither explained my alleged crime, nor revealed where they were taking me. Although they proceeded to search the vehicle from which they bundled me, they did not produce a search warrant. They dumped me into one of their three vehicles and drove circuitously around Kampala city; sometimes stopping adjacent to police stations and then moving on. After three hours of aimless driving, they sped to Kira Division Police Station where I was locked up in a cell for three nights. On the evening of 9th April 2017, in the presence of my legal team (comprising Nicholas Opiyo, Sheillah Nyanzi, Lilian Drabo and Shawn Mubiru), I underwent the routine Charge and Caution procedure in which the first charge sheet read to me was solely focused on the crime of soliciting for money from the public using the internet in contravention to the law which requires notifying the police before undertaking any fundraising. These allegations were based on a fundraising drive that I started on my Facebook timeline, inviting concerned citizens to contribute financially and in kind towards the #Pads4GirlsUg campaign aimed at distributing menstrual hygiene materials (including soap, re-useable and disposable sanitary pads) to school-girls in Uganda. The campaign to collect and distribute sanitary pads was a direct challenge to both President Museveni's failed promise made during elections campaigns, and the First Lady's declaration that government lacked money to provide the promised sanitary pads. After the charges were read to me, I chose not to say anything in my statement to the police officers. On 10th April 2017, amidst tight security, I was arraigned before the chief magistrate at Buganda Road Court to begin my incredible experience with the judicial system in a repressive military dictatorship.

Twists and Turns of #PairOfButtocks Criminal Case

This criminal case was allocated to Chief Magistrate James Ereemye Mawanda. The state (office of the Director of Public Prosecutions) was represented by Resident State Attorney Jonathan Muwaganya. My defense counsel comprised Nicholas Opiyo, Isaac Semakadde, Julius Galisonga, Lilian Drabo and Eron Kiiza. Within a courtroom jam-packed with local and foreign journalists, uniformed and plain-clothed security personnel, human rights defenders, social media activists, family, friends and supporters, the revised charges of cyber harassment and offensive communication were read to me. However, before the Chief Magistrate proceeded to ask me about how I pleaded, the

Dr. Stella Nyanzi in court.

SOURCE: https://cs.mg.co.za

state prosecutor hijacked the court processes by introducing what he termed as a pre-plea-taking application for the court to subject me to involuntary mental examination in accordance with the Mental Treatment Act (1938). Court adjourned for a short interlude, in order for the magistrate to examine the new application for mental examination. Thereafter, I pleaded 'Not Guilty' to both charges of cyber harassment and offensive communication of the president. My legal team expected to proceed with the application for release on bail. However, under undue pressure to impress the state, the magistrate refused to hear my application for bail. Instead, he proceeded to remand me to maximum security prison until 25th April 2017. In utter disbelief, I boarded the maroon prison bus – with several other accused and sentenced persons – and made my way to Luzira Women's Prison where I was to spend the next thirty-three days of my life.

Unbeknownst to me, on 11th April 2017, my legal team wrote an application to the Registrar of the High Court, seeking for revision of the proceedings against me in the lower court – specifically questioning the justice in the magistrate's refusal to hear my bail application, as well as seeking guidance about whether the trial should proceed under the Magistrates Courts Act and the Computer Misuse Act, rather than relying on an application invoking the archaic Mental Treatment Act. The deputy registrar of the Criminal Division of the High Court, Eleanor Khainza, summoned for my case file, as well as updated notes of the trial proceedings. The case was assigned to Justice Elizabeth Kabanda and scheduled for 26th April 2017.

On 24th April 2017, Nicholas Opiyo of Chapter Four Uganda and Wade McMullen of Robert F. Kennedy Human Rights submitted a joint petition to the United Nations Working Group on Arbitrary Detention regarding this case.

On 25th April 2017, when I appeared before the lower court, all parties agreed that in light of the pending guidance and ruling from the High Court, the case would only come up for mention. Court was adjourned to 10th May 2017.

Drumming up the most elaborate drama and fanfare, Justice Elizabeth Kabanda ordered all journalists and other public media workers to be barred from attending the proceedings in the High Court. Rather than hear the submissions of my legal team in a courtroom open to the public, she chose to hold closed-door hearings in her tiny chambers which could hardly accommodate the entirety of my enlarged legal team which was buffered up by additional counsel. In the absence of written submissions, she allocated the lawyers only five minutes in which to make their oral submissions. In spite of their elaborate preparations, only two of the lawyers were allowed the opportunity to speak in that time. She adjourned the session until 03:30PM, when she would give her ruling. Given the congestion of the session in her chambers, as well as the public interest in the proceedings, the defense team requested for relocation to one of the many available open courtrooms. In her High Court Ruling No. 9 of 2017, Justice Elizabeth Kabanda sent the case back to the lower court, directed the magistrate to expeditiously handle my bail application, and also insisted that the magistrate has power to hear the application for mental examination under the Mental Treatment Act. I returned to maximum security prison.

Although I was physically weak from illness, diagnosed with and treated for severe malaria by the prison health workers, I appeared at Buganda Road Magistrates Court on 10th May 2017. This time around, the magistrate entertained my application for bail and was physically introduced to my five sureties – namely Dr. Moses Khisa, Ms. Solome Nakaweesi-Kayondo, Ms. Sheillah Nyanzi, Mr. Geoffrey Wokulira Ssebaggala, and Ms. Annet Nana. The state prosecutor belaboured to make a case for the need for the court to subject me to mental examination and requisite mental treatment, prior to granting me bail. The prosecutor also attempted to advise the magistrate to condition my release on bail upon restricting my freedom of expression and social media writings particularly insisting that I should be barred from writing about members of the president's household. Ignoring these arguments, I was released on bail and given non-cash court bond of ten million Uganda Shillings. Court was adjourned to 25th May 2017.

The prosecutor also attempted to advise the magistrate to condition my release on bail upon restricting my freedom of expression and social media writings particularly insisting that I should be barred from writing about members of the president's household.

In the period immediately after my release on bail, a new legal team was constituted upon receiving my written instructions to 1) petition the Constitutional Court against articles in the Mental Treatment Act that contravene several rights provided for in the constitution, 2) submit an application to the Chief Magistrate to halt the mental examination procedure arising out of the Mental Treatment Act – pending the ruling on the petition, and 3) proceed with the hearing and trial of the criminal case arising out of the Computer Misuse Act. On 25th May 2017, my new legal team under the leadership of Constitutional Law expert Peter Walubiri introduced Constitutional Court Petition No. 18 of 2017, *Stella Nyanzi v. Attorney General* and applied to the lower court to stay the state prosecutor's application to subject me to mental examination. Furthermore, my lawyers prayed that court proceeds with the hearing and trial of the criminal case in which I am charged with cyber harassment and offensive communication against the president. Court was adjourned to 7th June 2017.

Although copies of our submissions were previously given to the state prosecutor, on 7th June 2017 Resident State Attorney Jonathan Muwaganya denied having received the same documents, and asked the court to give him more time to examine both the Constitutional Petition and the application to the lower court to halt the proceedings of the mental examination application. In spite of protestations from my defense lawyers, the Chief Magistrate agreed to give the state prosecutor two weeks to read the documents and prepare his rebuttal. Disappointed about the gimmicks of legal professionals wasting the time of court, I wrote about the state prosecutor's

sloppiness, tardiness and underhandedness on my Facebook timeline. I decried the blatant waste of public resources contained within the audacity of a public official coming to court without preparing by reading documents provided for a hearing.

A new twist was introduced into the court hearing on the morning of 20th June 2017. Full of renewed gusto, the state prosecutor asked the Chief Magistrate to cancel my release on bail because he alleged that I violated the subjudice rule in my social media writings about the case. Submitting copies of my Facebook posts about his previous performance in court, he argued that I had violated a condition of my bail – namely that I should not publicly discuss the merits and weaknesses of the case. My legal team combated all the new allegations. After a break, the Chief Magistrate gave his ruling in which he maintained my bail and also temporarily stayed the state prosecutor's application for me to be subjected to mental examination pending the Constitutional Court's ruling on my petition against the constitutionality of the provisions of the Mental Treatment Act. Importantly, in this ruling, the Chief Magistrate distinguished between violating the subjudice rule and writing to complain about the inadequacies of court procedures or personnel.

In the following court session of 21st July 2017, my defense lawyers requested that the state prosecutor produces both the evidence and witnesses to my alleged crimes of cyber harassment and offensive communication against the president. The state prosecutor insisted that it was his understanding that court was waiting for the ruling of the Constitutional Court about my petition against the Mental Treatment Act. Furthermore, he insisted again about the need for me to be subjected to mental examination and requisite treatment before proceeding with the court hearing. My defense lawyers countered this by distinguishing between the mental healthcare procedures arising out of the Mental Treatment Act, on the one hand, and the court hearing procedures arising out of the Computer Misuse Act. We asked court to proceed with the examination and cross-examination of witnesses and their evidence, or else dismiss the charges as baseless. In response, the state prosecutor asked for more time to consult the Director of Public Prosecutions (DPP) about how to proceed. Given that the state prosecutor received his instructions from the DPP, the Chief Magistrate granted him the time for these consultations. Court was adjourned to 21st August 2017.

On two consecutive pre-scheduled dates of 21st August 2017 and 21st September 2017, in spite of the state prosecutor and my defense counsel attending on time, the Chief Magistrate neither showed up to court nor gave any explanations for this absence. The hearing was adjourned to 23rd October 2017 – a day when state prosecutors were on strike against poor working conditions. Thus courts were not working. Court was adjourned to 24th November 2017.

Although the ongoing local court proceedings have been drawn out because of undue delays caused by either an absent Chief Magistrate or an absent state prosecutor, the case received a decision at the international level. The United Nations Working Group on Arbitrary Detention gave a decision in favour of freedom of expression online, determined that I was arbitrarily detained for my Facebook posts criticizing the president, and proposed several remedies[1].

Conclusion

Although the #PairOfButtocks case was not the first criminal case in Uganda to arise out of the Computer Misuse Act, it gained notoriety because of the colourful language of discussion and debate that it generated on both the public and social media in Uganda, Africa and the world at large. The disproportionate severity of reprisals and pre-trial penalties meted out by the state – specifically the arbitrary pre-trial detention on remand for thirty-three days, denial to hear an application for bail, and application for involuntary mental examination of the accused – highlighted how this was political scape-goating aimed at controlling, intimidating and deterring other oppositional voices criticising the leadership of President Yoweri Museveni. However, rather than halt the criticisms on the internet and in the public media, this criminal case generated new frontiers of further engaged critique. Arising out of this criminal case, a petition was filed challenging the constitutionality of some of the provisions of the Mental Treatment Act. Although it was filed in June 2017, no hearing date has yet been assigned to this Constitutional Court petition. It is good that another Constitutional Petition was filed challenging provisions of the Computer Misuse Act that are being employed by the state to quell dissent (*Andrew Karamagi & Robert Shaka v Attorney General*).[2] Furthermore, a petition was filed to the United Nations Working Group on Arbitrary Detention which decided that I was arbitrarily detained using a veneer of law which is in conflict with international human rights that protect freedom of expression.

1 A/HRC/WGAD/2017/57 Opinion no. 57/2017 concerning Stella Nyanzi (Uganda).

2 *Andrew Karamagi&Robert Shaka v Attorney General*,Constitutional Petition No. 5 of 2016.

CASE UPDATE

The case of *Uganda v Robert Shaka*

On June 8th 2015, Mr. Robert Shaka was arrested by a group of about 10 policemen. He was taken to the Special Investigations Unit headquarters and told that the reasons for his arrests were the following:

> i) *That using computers and other electronic devices, he issued offensive communications against the sovereign state of Uganda, bringing it into hatred and contempt and accordingly committing the offence of promotion of sectarianism contrary to section 41 of the Penal Code Act.*
>
> ii) *That using computers and other electronic devices, he used offensive communication against President Yoweri Museveni, Janet Museveni, Kale Kayihura, a one "Mbabazi" and a one "Kelen" thereby committing the offence of offensive communication contrary to Section 25 of the Computer Misuse Act.*

For a long time, it has been suspected that Mr. Shaka is Tom Voltaire Okwalinga. He has been persistently persecuted by police since February 2015. On June 11th 2015, Mr. Shaka was produced before Buganda Road Magistrates Court and charged with the offence of offensive communication under Section 25 of the Computer Misuse Act. The particulars of the charge were that:

> *'Mr. Shaka, disguising himself as Tom Voltaire Okwalinga (TVO), between 2011 and 2015, willfully and repeatedly using a computer, with no purpose of legitimate communication, disturbed the right of privacy of President Museveni by posting statements as regards to his health condition on social media, to wit, Facebook.'*

Mr. Shaka was granted bail by the Magistrates Court but the hearing of the case never took place. On February 3rd 2016, Robert Shaka and Andrew Karamagi filed a Petition in the Constitutional Court challenging the constitutionality of Section 25 of the Computer Misuse Act, the Section Mr. Shaka was charged under. His lawyers applied to court for a stay of the criminal proceedings, which was granted on 22nd April 2016, pending determination of the Constitutional Petition.

The Constitutional Petition

On February 3rd 2016, Robert Shaka and Andrew Karamagi filed a petition challenging the constitutionality of Section 25 of the Computer Misuse Act.[1] In their Petition, the two contend that the section, which declares it an offence for any person to 'willfully and repeatedly use electronic communication to disturb or attempt to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication' is inconsistent with and in contravention of Article 29(1)(a) of the Constitution. They also state that the section is an insidious form of censorship, which restricts the free flow of opinions and ideas essential to sustain the collective life of the citizenry in the digital age; it is vague and overly broad; and that there is no evidence that Government could not achieve the intended purpose with less drastic measures.

They then ask court to make a declaration that the section is inconsistent with or in contravention of Article 29(1)(a) of the Constitution and is to that extent null and void. They also ask the Court to direct the Director of Public Prosecutions to stay the prosecution of all and any citizens currently on trial for violating the section and an order staying the enforcement of the section or similar provisions of the law, which disproportionately curtail enjoyment of the freedom of speech and expression by citizens.

The Attorney General filed a response to the Petition and contended that the Petition does not raise any questions for Constitutional interpretation and is thus devoid of any merit. The response also argues that section 25 of the computer Misuse Act is not inconsistent with or in contravention of Articles 29(1)(a) of the Constitution, and that the Petitioners are not entitled to the declarations sought.

1 *Andrew Karamagi & Robert Shaka v Attorney General*, Constitutional Petition No. 5 of 2016.

APPENDICES

1. HRAPF' STATEMENT ON THE PROSECUTION OF DR. STELLA NYANZI

Plot 390 Prof. Apolo Nsibambi Road, Namirembe, Kampala.
P. O. Box 25603, Kampala.
Tel: +256-414-530683/+256-312-530683
Email: info@hrapf.org. Website: www.hrapf.org

Kampala, Thursday 13 April 2017

THE COMPUTER MISUSE ACT SHOULD NOT BE MISUSED TO GAG FREE EXPRESSION IN UGANDA

On the night of 7th April 2017, Makerere University researcher Dr. Stella Nyanzi was kidnapped by state agents who after driving her around the city for hours eventually took her to Kiira Police Division where she was detained. She was then produced before the Buganda Road Chief Magistrate on 10th April, and charges of cyber harassment and offensive communications under sections 24(1) and (2)(a), and 25 of the Computer Misuse Act of 2011 respectively were read to her. She pleaded not guilty to both charges, and was remanded to Luzira Prison until 25th April 2015.

Dr. Nyanzi's arrest and prosecution arises from her posts on the social media site Facebook, in which she used colourful and poetic language with sexual metaphors to criticise the President, his wife and the government for misrule, and for failed pledges. This attracted the offensive communications charge. Her 28th January 2017 post in which she referred to the President as a 'pair of buttocks' was specifically pointed out and used as the basis for the offensive communications charge.

The Computer Misuse Act, 2011 was enacted partly to ensure the 'safety and security of electronic transactions and information systems' and to prevent 'abuse or misuse of information systems including computers' which are both noble objectives. However, section 24(1) and (2)(4) and section 25 are being misused. Section 24(1) criminalises cyber harassment which is in part defined in section 24(2)(a) as 'making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent'. These provisions are becoming increasingly popular to deal with any behaviour regarded as morally inappropriate. Since the Act came into force, HRAPF has recorded two cases where these provisions were used against people regarded as 'immoral' because of their behaviour, work, sexual orientation or gender identity. The Constitution, which is Uganda's supreme law in Article 29(1)(a) guarantees the freedom of speech and expression which includes freedom of the press and other media. According to the Supreme Court of Uganda, the speech and expression protected extends to that which offend, shock and disturb. Indeed, the Constitution provides for a limitation on all rights including the right to freedom of expression. Article 43(5) provides that 'no person shall prejudice the fundamental or other human rights and freedoms of others or the public interest.' However, article 43(6) provides that the public interest shall not permit, among others: political persecution, and any limitation of the enjoyment of the rights and freedoms prescribed by this Chapter beyond what is acceptable and demonstrably justifiable in a free and democratic society. In interpreting this provision, the Supreme Court found that it was a 'limitation within a limitation' and that it is the right that had to be given prominence. Therefore, speech that involves discussion of sex, sexual orientation or gender identity or sexual acts should not necessarily be limited simply because it is regarded by the majority as being 'obscene, lewd, lascivious or indecent.' Again, these statements were made by a self-declared supporter of the political opposition in the context of criticising government decisions. All the messages mentioned in the charge contain legitimate political

concerns despite the choice of language. Therefore arresting her for such speech amounts to political persecution. This provision therefore falls short of constitutional standards, and ought to be repealed.

Section 25 criminalises the wilful and repeated use of 'electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person without purpose of legitimate communication.' The facts of Dr. Nyanzi's case do not support such a charge. The statement cannot be said to have disturbed the 'peace, quiet or right of privacy' of any person and more so the President. The President is in a position where criticism and public discussion of all aspects of his personal and political life can be expected. The communication was clearly made with a purpose of political comment, and so cannot be said to have been made 'without purpose.'

Therefore the Computer Misuse Act, which has such good intentions, is now becoming the new legal basis for policing morals and sacrificing the gem of freedom of expression. Usually, issues of defamation are dealt with under the realm of tort law. A person who feels that he or she has been harassed or defamed is free to institute civil proceedings against the perpetrator. Using the criminal law to fight political battles and to save face by public figures is an abuse of court process and a waste of scarce state resources. Nothing stops the President from bringing a civil action against Dr. Nyanzi if he feels insulted and defamed.

HRAPF therefore calls upon the state to:

1. Stop the misuse of the Computer Misuse Act by applying it only where it is appropriate and not for harassing political opponents and unpopular minorities.

2. Review section 24(2)(a) of the Computer Misuse Act which only restricts speech and expression on the basis that it is 'obscene, lewd, lascivious or indecent'; something that limits freedom of speech beyond the constitutional parameters.

3. Drop the unconstitutional and trumped up charges against Dr. Stella Nyanzi.

Taking human rights to all

2. FULL TEXT OF THE COMPUTER MISUSE ACT

ACTS
SUPPLEMENT No. 2 **14th Febuary, 2011.**

ACTS SUPPLEMENT

to The Uganda Gazette No. 10 Volume CIV dated 14th February, 2011.

Printed by UPPC, Entebbe, by Order of the Government.

Act 2 *Computer Misuse Act* **2011**

THE COMPUTER MISUSE ACT, 2011.

ARRANGEMENT OF SECTIONS.

PART I—PRELIMINARY.

Section.

PART II—GENERAL PROVISIONS.

PART III—INVESTIGATIONS AND PROCEDURES.

PART IV—COMPUTER MISUSE OFFENCES.

Section.

THE COMPUTER MISUSE ACT, 2011

An Act to make provision for the safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic transactions in a trustworthy electronic environment and to provide for other related matters.

DATE OF ASSENT: 1st November, 2010.

Date of Commencement: See Section 1.

BE IT ENACTED by Parliament as follows:

PART I—PRELIMINARY.

1. Commencement.

This Act shall come into force on a date appointed by the Minister by statutory instrument

2. Interpretation.

In this Act, unless the context otherwise requires—

"access" means gaining entry to any electronic system or data held in an electronic system or causing the electronic system to perform any function to achieve that objective;

"application" means a set of instructions that, when executed in a computer system, causes a computer system to perform a function and includes such a set of instructions held in any removable storage medium which is for the time being in a computer system;

"authorised officer" has the meaning assigned to it in section 28;

"child" means a person under the age of eighteen years;

"computer" means an electronic, magnetic, optical, electrochemical or other data processing device or a group of such interconnected or related devices, performing logical, arithmetic or 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;

"computer output" or "output" means a statement, information or representation, whether in written, printed, pictorial, graphical or other form—

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced from a computer;

"computer service" includes computer time, data processing and the storage retrieval of data;

"content" includes components of computer hardware and software;

"currency point" means the value of a currency point specified in the Schedule;

"damage" means any impairment to a computer or the integrity or availability of data, program, system or information that—

(a) causes any loss;

(b) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons;

(c) causes or threatens physical injury or death to any person; or

(d) threatens public health or public safety;

"data" means electronic representations of information in any form;

"data message" means data generated, sent, received or stored by computer means; and includes—

(a) voice, where the voice is used in an automated transaction; and

(b) a stored record;

"electronic device", "acoustic device", or "other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"electronic record" means data which is recorded or stored on any medium in or by a computer or other similar device, that can be read or perceived by a person or a computer system or other similar device and includes a display, printout or other out put of that data;

"function" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system;

"information system services" includes a provision of connections, operation facilities, for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service;

"intercept", in relation to a function of a computer, includes listening to or recording a function of a computer or acquiring the substance, meaning or purport of such a function;

"Minister" means the Minister responsible for information and communications technology;

"person" includes any company or association or body of persons corporate or unincorporate;

"program" or "computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function;

"traffic data" means any computer data relating to communication by means of a computer system generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service.

PART II—GENERAL PROVISIONS.

3. Securing access.

A person secures access to any program or data held in a computer if that person—

(a) views, alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses or destroys it; or

(d) causes it to be output from the computer in which it is held whether by having it displayed or in any other manner.

4. Using a program.

A person uses a program if the function he or she causes the computer to perform—

(a) causes the program to be executed; or

(b) is itself a function of the program.

5. Authorised access.

Access by a person to any program or data held in a computer is authorised if—

(a) the person is entitled to control access to the program or data in question; or

(b) the person has consent to access that program or data from any person who is charged with giving that consent.

6. References.

(1) A reference to a program or data held in a computer includes a reference to any program or data held in any removable storage medium and a computer may be regarded as containing any program or data held in any such medium.

(2) A reference to a program includes a reference to part of a program.

7. Modification of contents.

A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer connected to it result into—

(a) a program, data or data message held in the computer concerned being altered or erased; or

(b) a program, data or data message being added to its contents.

8. Unauthorised modification.

Modification is unauthorised if—

(a) the person whose act causes it, is not entitled to determine whether the modification should be made; and

(b) he or she does not have consent to the modification from a person who is entitled.

PART III—INVESTIGATIONS AND PROCEDURES.

9. Preservation Order.

(1) 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.

(2) For the purpose of subsection (1), data includes traffic data and subscriber information.

(3) An order made under subsection (1) shall remain in force—

(a) until such time as may reasonably be required for the investigation of an offence; or

(b) where prosecution is instituted, until the final determination of the case or until such time as the court deems fit.

10. Disclosure of preservation Order.

The investigative officer may, for the purpose of a criminal investigation or the prosecution of an offence, apply to court for an order for the disclosure of—

(a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data; or

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or electronic key enabling access to or the interpretation of data.

11. Production Order.

(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigative officer may apply to court for an order compelling—

(a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and

(b) any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material to which an investigation relates consists of data stored in a computer, computer system or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

PART III—COMPUTER MISUSE OFFENCES.

12. Unauthorised access.

(1) A person who intentionally accesses or intercepts any program or data without authority or permission to do so commits an offence.

(2) A person who intentionally and without authority to do so, interferes with data in a manner that causes the program or data to be modified, damaged, destroyed or rendered ineffective, commits an offence.

(3) A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component which is designed primarily to overcome security measures for the protection of data or performs any of those acts with regard to a password, access code or any other similar kind of data, commits an offence.

(4) A person who utilises any device or computer program specified in subsection (3) in order to unlawfully overcome security measures designed to protect the program or data or access to that program or data, commits an offence.

(5) A person who accesses any information system so as to constitute a denial including a partial denial of service to legitimate users commits an offence.

(6) The intent of a person to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(7) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

13. Access with intent to commit or facilitate the commission of a further offence.

(1) A person who commits any acts specified under section 12 with intent to—

(a) commit any other offence; or

(b) facilitate the commission of any other offence,

commits an offence.

(2) The offence to be facilitated under subsection (1)(b) may be one committed by the person referred to in subsection (1) or by any other person.

(3) It is immaterial for the purposes of this section whether the act under this section is committed on the same occasion as the offence under section 12 or on any future occasion.

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

14. Unauthorised modification of computer material.

(1) A person who—

(a) does any act which causes an unauthorised modification of the contents of any computer; and

(b) has the requisite intent and the requisite knowledge at the time when he or she does the act,

commits an offence.

(2) For the purposes of subsection (1)(b) the requisite intent is an intent to cause a modification of the contents of any computer and by doing so—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

(3) The intent under subsection (1)(b) need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) the requisite knowledge is knowledge that any modification that the person intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind specified in subsection (2) is intended to be permanent or temporary.

(6) A person who commits an offence under this section is liable on conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

15. Unauthorised use or interception of computer service.

(1) Subject to subsection (2), a person who knowingly—

(a) secures access to any computer without authority for the purpose of obtaining, directly or indirectly, any computer service;

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device whether similar or not; or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence is liable to a fine not exceeding one hundred and sixty eight currency points or imprisonment not exceeding seven years or both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

16. Unauthorised obstruction of use of computer.

A person who, knowingly and without authority or lawful excuse—

(a) interferes with or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to or impairs the usefulness or effectiveness of any program or data stored in a computer,

commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

17. Unauthorised disclosure of access code.

(1) A person who knowingly and without authority discloses any password, access code or any other means of gaining access to any program or data held in any computer knowing or having reason to believe that it is likely to cause loss, damage or injury to any person or property, commits an offence.

(2) A person who commits an offence under subsection (1) is liable on conviction to a fine not exceeding two hundred and forty currency points or to imprisonment not exceeding ten years or both; and in the case of a subsequent conviction, to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

18. Unauthorised disclosure of information.

(1) Except for the purposes of this Act or for any prosecution for an offence under any written law or in accordance with an order of court, a person who has access to any electronic data, record, book, register, correspondence, information, document or any other material, shall not disclose to any other person or use for any other purpose other than that for which he or she obtained access.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment not exceeding ten years or both.

19. Electronic fraud.

(1) A person who carries out electronic fraud commits an offence and is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

(2) For the purposes of this section "electronic fraud" means deception, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both.

20. Enhanced punishment for offences involving protected computers.

(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 12, 14, 15 or 16, the person convicted of an offence is, instead of the punishment prescribed in those sections, liable on conviction, to imprisonment for life.

(2) For the purposes of subsection (1), a computer is treated as a "protected computer" if the person committing the offence knows or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for—

(a) the security, defence or international relations of Uganda;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities or public key infrastructure; or

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2).

21. Abetment and attempts.

(1) A person who abets another person in committing an offence under this Act, commits that offence and is liable on conviction to the punishment prescribed for the offence.

(2) Any person who attempts to commit any offence under this Act commits that offence and is liable on conviction to the punishment prescribed for the offence.

22. Attempt defined.

(1) When a person, intending to commit an offence, begins to put his or her intention into execution by means adapted to its fulfillment, and manifests his or her intention by some overt act, but does not fulfill his or her intention to such an extent as to commit the offence, he or she is deemed to attempt to commit the offence.

(2) It is immaterial—

(a) except so far as regards punishment, whether the offender does all that is necessary on his or her part for completing the commission of the offence, or whether the complete fulfillment of his or her intention is prevented by circumstances independent of his or her will, or whether the offender desists of his or her own motion from the further prosecution of his or her intention; or

(b) that by reason of circumstances not known to the offender it is impossible in fact to commit the offence.

23. Child pornography.

(1) A person who—

(a) produces child pornography for the purposes of its distribution through a computer;

(b) offers or makes available child pornography through a computer;

(c) distributes or transmits child pornography through a computer;

(d) procures child pornography through a computer for himself or herself or another person; or

(e) unlawfully possesses child pornography on a computer,

commits an offence.

(2) A person who makes available pornographic materials to a child commits an offence.

(3) For the purposes of this section "child pornography" includes pornographic material that depicts—

(a) a child engaged in sexually suggestive or explicit conduct;

(b) a person appearing to be a child engaged in sexually suggestive or explicit conduct; or

(c) realistic images representing children engaged in sexually suggestive or explicit conduct.

(4) A person who commits an offence under this section is liable on conviction to a fine not exceeding three hundred and sixty currency points or imprisonment not exceeding fifteen years or both.

24. Cyber harassment.

(1) A person who commits cyber harassment is liable on conviction to a fine not exceeding seventy two currency points or imprisonment not exceeding three years or both.

(2) For purposes of this section cyber harassment is the use of a computer for any of the following purposes—

(a) making any request, suggestion or proposal which is obscene, lewd, lascivious or indecent;

(b) threatening to inflict injury or physical harm to the person or property of any person; or

(c) knowingly permits any electronic communications device to be used for any of the purposes mentioned in this section.

25. Offensive communication.

Any person who willfully and repeatedly uses electronic communication to disturb or attempts to disturb the peace, quiet or right of privacy of any person with no purpose of legitimate communication whether or not a conversation ensues commits a misdemeanor and is liable on conviction to a fine not exceeding twenty four currency points or imprisonment not exceeding one year or both.

26. Cyber stalking.

Any person who willfully, maliciously, and repeatedly uses electronic communication to harass another person and makes a threat with the intent to place that person in reasonable fear for his or her safety or to a member of that person's immediate family commits the crime of cyber stalking and is liable on conviction to a fine not exceeding one hundred and twenty currency points or imprisonment not exceeding five years or both.

27. Compensation.

Where a person is convicted under this Act, the court shall in addition to the punishment provided therein, order such person to pay by way of compensation to the aggrieved party, such sum as is in the opinion of the court just, having regard to the loss suffered by the aggrieved party; and such order shall be a decree under the provisions of the Civil Procedure Act, and shall be executed in the manner provided under that Act.

PART V—MISCELLANEOUS.

28. Searches and seizure.

(1) Where a Magistrate is satisfied by information given by a police officer that there are reasonable grounds for believing—

(a) that an offence under this Act has been or is about to be committed in any premises; and

(b) that evidence that such an offence has been or is about to be committed is in those premises,

the Magistrate may issue a warrant authorising a police officer to enter and search the premises, using such reasonable force as is necessary.

(2) An authorised officer may seize any computer system or take any samples or copies of applications or data—

(a) that is concerned in or is on reasonable grounds believed to be concerned in the commission or suspected commission of an offence, whether within Uganda or elsewhere;

(b) that may afford evidence of the commission or suspected commission of an offence, whether within Uganda or elsewhere; or

(c) that is intended to be used or is on reasonable grounds believed to be intended to be used in the commission of an offence.

(3) A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, only by virtue of a search warrant.

(4) The provisions of section 71 of the Magistrates Court's Act apply with the necessary modifications to the issue and execution of a search warrant referred to in subsection (3).

(5) An authorised officer executing a search warrant referred to in subsection (3), may—

(a) at any time search for, have access to and inspect and check the operation of any computer system, application or data if that officer on reasonable grounds believes it to be necessary to facilitate the execution of that search warrant;

(b) require a person having charge of or being otherwise concerned with the operation, custody or care of a computer system, application or data to provide him or her with the reasonable assistance that may be required to facilitate the execution of that search warrant; and

(c) compel a service provider, within its existing technical capability—

(i) to collect or record through the application of technical means; or

(ii) to co-operate and assist the competent authorties in the collection or recording of traffic data in real time, associated with specified communication transmitted by means of a computer system.

(6) In seizing any computer system or taking any samples or copies of applications or data or performing any of the actions referred to in subsection (5), an authorised officer shall have due regard to the rights and interests of a person affected by the seizure to carry on his or her normal activities.

(7) A person who obstructs, hinders or threatens an authorised officer in the performance of his or her duties or the exercise of his or her powers under this section commits an offence and is liable on conviction to a fine not exceeding twelve currency points or imprisonment not exceeding six months or both.

(8) A computer system seized or samples or copies of applications or data taken by the authorised officer shall be returned within seventy two hours unless the authorised officer has applied for and obtained an order in an inter party application for extension of the time.

(9) In this section—

"authorised officer" means a police officer who has obtained an authorising warrant under subsection (1); and

"premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hover craft.

29. Admissibility and evidential weight of a data message or an electronic record.

(1) In any legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of a data message or an electronic record—

(a) merely on the ground that it is constituted by a data message or an electronic record;

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain; or

(c) merely on the ground that it is not in its original form.

(2) A person seeking to introduce a data message or an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

(3) Subject to subsection (2), where the best evidence rule is applicable in respect of an electronic record, the rule is satisfied upon proof of the authenticity of the electronic records system in or by which the data was recorded or stored.

(4) When assessing the evidential weight of a data message or an electronic record, the court shall have regard to—

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the authenticity of the data message was maintained;

(c) the manner in which the originator of the data message or electronic record was identified; and

(d) any other relevant factor.

(5) The authenticity of the electronic records system in which an electronic record is recorded or stored shall, in the absence of evidence to the contrary, be presumed where—

(a) there is evidence that supports a finding that at all material times the computer system or other similar device was operating properly or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic record and there are no other reasonable grounds on which to doubt the authenticity of the electronic records system;

(b) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

(6) For the purposes of determining whether an electronic record is admissible under this section, evidence may be presented in respect of any set standard, procedure, usage or practice on how electronic records are to be recorded or stored, with regard to the type of business or endeavours that used, recorded or stored the electronic record and the nature and purpose of the electronic record.

(7) For the avoidance of doubt, this section does not modify the common law or a statutory rule relating to the admissibility of records, except the rules relating to authentication and best evidence.

30. Territorial jurisdiction.

(1) Subject to subsection (2), this Act shall have effect, in relation to any person, whatever his or her nationality or citizenship and whether he or she is within or outside Uganda.

(2) Where an offence under this Act, is committed by any person in any place outside Uganda, he or she may be dealt with as if the offence had been committed within Uganda.

(3) For the purposes of this Act, this section applies if, for the offence in question—

(a) the accused was in Uganda at the material time; or

(b) the computer, program or data was in Uganda at the material time.

31. Jurisdiction of courts.

A court presided over by a chief magistrate or magistrate grade I has jurisdiction to hear and determine all offences in this Act and, notwithstanding anything to the contrary in any written law, has power to impose the full penalty or punishment in respect of any offence under this Act.

32. Power of Minister to amend Schedule

The Minister may by statutory instrument with the approval of the Cabinet, amend the Schedule to this Act.

SCHEDULE

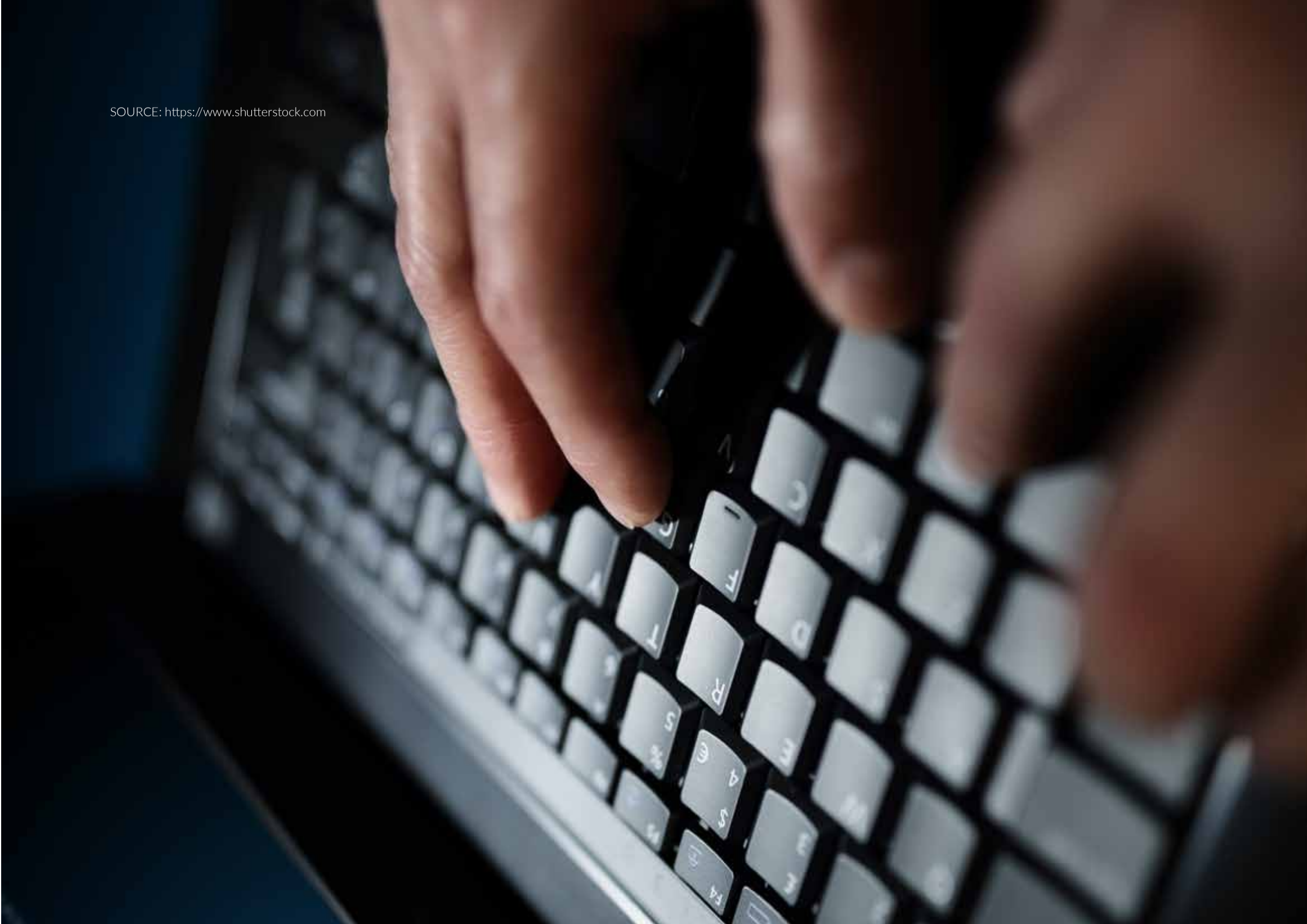
Section 2.

Currency point

One currency point is equivalent to twenty thousand shillings.

Cross reference

Magistrates Courts Act, Cap.16.



SOURCE: https://www.shutterstock.com

Human Rights Awareness and Promotion Forum (HRAPF)

Plot 390 Prof. Apolo Nsibambi Road,
Namirembe, Kampala

P. O. Box 25603, Kampala.

Telephone:+256-414-530683

Email:info@hrapf.org

Website:www.hrapf.org

Facebook:hrapf.uganda

Twitter:@hrapf_uganda