AFRICAN HUMAN RIGHTS LAW JOURNAL

To cite: R Kakungulu-Mayambala & S Rukundo 'Digital activism and free expression in Uganda' (2019) 19 *African Human Rights Law Journal* 167-192
http://dx.doi.org/10.17159/1996-2096/2019/v19n1a9

Digital activism and free expression in Uganda

*Ronald Kakungulu-Mayambala**
Associate Professor, Human Rights and Peace Centre (HURIPEC), School of Law, Makerere University, Kampala, Uganda
https://orcid.org/0000-0002-1161-365X

*Solomon Rukundo***
Researcher, Mawazo Policy Institute, Kampala, Uganda
https://orcid.org/0000-0002-6257-7070

Summary

In recent years in Africa there has been increasing use of digital technologies in terms of political and social activism. In Uganda this takes the form of text messaging, social media activism, blogging and, in some cases, hacktivism. This article examines digital activism in Uganda in light of the guarantee of freedom of expression under international instruments and the Ugandan Constitution. The article begins with an analysis of international and regional instruments that buttress digital activism through their enunciations regarding freedom of expression. The article then takes a critical look at a number of laws, such as the Computer Misuse Act, the Anti-Terrorism Act and the Regulation of Interception of Communications Act, that directly or indirectly restrict digital activism. The article argues that for free expression to be fully exercised in the online environment, laws and policies with provisions in conflict with the Constitution and international instruments will have to be amended or abolished.

Key words: *digital activism; freedom of expression; Uganda; internet; digitalisation*

* LLB (Hons) (Makerere) LLM (Fordham) SJD (Arizona); rmkakungulu@gmail.com
** LLB (Hons) (Dar es Salaam); soloruk12@gmail.com

1 Introduction

The internet increasingly is becoming a part of our everyday lives. Currently 24,4 per cent of the population on the African continent is estimated to have access to the internet.[1] More people on the continent are gaining access through the proliferation of affordable internet-enabled smartphones. In Uganda, the number of internet users was estimated to be 18,5 million individuals as of June 2018.[2]

In Africa the internet is considerably more politicised than in other parts of the world. Tools such as social media undoubtedly are altering the way in which activism is carried out. These tools facilitate networking, making the mobilisation of people for social or political causes much easier.[3] A study by a United States (US) company, Portland Communications, on the use of the social media platform Twitter in Africa found that in 2018 almost half of the most popular African hash-tags related to political issues.[4] Ugandans, like their African counterparts, use the internet and other electronic technologies to engage in various forms of activism. Activism through electronic technologies takes the form of text messaging on mobile phones,[5] blogging,[6] on-line petitions,[7] social media posts, and the sharing of video recordings.[8]

1 'ITU releases 2018 global and regional ICT estimates' ITU Press Release, https://www.itu.int/en/mediacentre/Pages/2018-PR40.aspx (accessed 8 March 2019).

2 UCC 'Post, broadcasting and telecommunications market and industry Q2 Report, 2017' (2018) 23.

3 DK Kalinaki 'How social media [are] transforming Uganda's political and social landscape' *African Centre for Media Excellence* 20 July 2016, https://acme-ug.org/2016/07/20/how-social-media-are-transforming-ugandas-political-and-social-landscape/ (accessed 16 December 2017).

4 Portland Communications 'How Africa tweets 2018', https://portland-communications.com/pdf/How-Africa-Tweets-2018.pdf (accessed 8 March 2019).

5 IPA 'The impact of a text messaging platform on government services in Uganda' (2016), https://www.poverty-action.org/study/impact-text-messaging-platform-government-services-uganda (accessed 8 March 2019). In 2013 the UN used a free, SMS-based citizen reporting system. We captured the views of more than 17 000 young people in a survey about the development priorities in their communities: O Kjørven 'Crowdsourcing the next global development agenda' *The Guardian* 7 May 2013, https://www.theguardian.com/media-network/media-network-blog/2013/may/07/united-nations-crowdsource-global-development (accessed 12 March 2019).

6 P Ampurire 'Blogging on a steady rise in Uganda' *Chimp Reports* 26 October 2015, https://chimpreports.com/feature-blogging-on-a-steady-rise-in-uganda/ (accessed 8 March 2019).

7 'Over 30 000 people sign an online petition to free Bobi Wine' *Dispatch* 22 August 2018, http://dispatch.ug/2018/08/22/30000-people-sign-online-petition-free-bobi-wine/ (accessed 8 March 2019).

8 'How social media has evolved in Uganda' *Daily Monitor* 2 July 2015, http://www.monitor.co.ug/artsculture/Reviews/How-social-media-has-evolved-in-Uganda/691232-2771872-cmhu0q/index.html (accessed 27 December 2017).

Digital activism has been defined as the reliance on digital tools to advocate and promote or impede political reform with the desire to effect improvements in society.[9] While digital activism often is associated with on-line action for political causes,[10] it can also be used for non-political activities. For example, in Uganda digital activism was used to encourage support for Miss Uganda, Quiin Abenakyo, when she was among the finalists in the 2018 Miss World competition.[11] Digital activism also has been used to do crowd funding for different causes, such as combating disease or paying the medical bills of patients.[12] Digital activism simply is the continuation of traditional grassroots mobilisation using modern digital tools as aids.

2 Forms and tools of digital activism

Vegh[13] classifies digital activism based on the initiative taken by the activist – whether the activist is sending out information, calling for action or initiating an action. He classifies digital activism into three main categories. The first is awareness or advocacy. Here public awareness is built by availing information relating to the cause in an easily accessible way. It focuses largely on events and issues that go unreported, underreported, or misreported among the mainstream news sources. In this way, a digital tool such as the internet is used as an alternative news and information source. Digital activism allows for campaigning for marginalised causes such as gay rights, which would otherwise be difficult to campaign for using traditional mainstream media. Social media platforms such as Facebook have been praised by gay rights activists in Uganda for providing them with a neutral platform where their voices can be heard.[14] Information is made

9 MB Chibita 'Digital activism in Uganda' in B Mutsvairo *Digital activism in the social media era: Critical reflections on emerging trends in sub-Saharan Africa* (2016) 69.

10 Eg, the *Encyclopaedia Britannica* defines it as using 'the internet and digital media as key platforms for mass mobilisation and political action'. MA Fuentes 'Digital activism' in *Encyclopaedia Britannica*, https://www.britannica.com/topic/digital-activism (accessed 8 March 2019).

11 P Ampurire 'Ugandans launch aggressive online campaign to vote Quiin Abenakyo for Miss World' *Soft Power News* 4 December 2018, https://www.softpower.ug/ugandans-launch-aggressive-online-campaign-to-vote-quiin-abenakyo-for-miss-world/ (accessed 8 March 2019).

12 Eg, in 2016 an aggressive online campaign raised UGX 300 million (US $86 000) for the cancer treatment of Carol Atuhairwe. E Aturinde 'Save Carol cancer drive exceeds target' *Daily Monitor*, https://www.monitor.co.ug/News/National/Save-Carol-cancer-drive-exceeds-target/688334-3189224-29si48/index.html (accessed 8 March 2019).

13 S Vegh 'Classifying forms of online activism: The case of cyber protests against the World Bank' in M McCaughey & D Ayers *Cyberactivism: Online activism in theory and practice* (2003) 71.

14 J Morgan 'Facebook slams fake report claiming it was pulling out of Uganda over anti-gay law' *Gay Star News*, http://www.gaystarnews.com/article/facebook-threatens-pull-out-uganda-over-anti-gay-law270214/#gs.C5aOPQ0 (accessed 16 December 2017).

available on-line, and when the public accesses this information awareness about the cause grows.

The second category is organisation or mobilisation. Digital tools can be used to call for action either on-line or off-line. Digital activism can be used to call for and organise off-line action. Here information regarding the date, time and venue of a demonstration or protest is communicated on-line. Digital activism can also be used to engage in an action that would have been possible off-line but which can be done more efficiently on-line. For example, people can engage with the Member of Parliament (MP) of their area on social media. The third category is action or reaction, which basically involves taking action for or against a cause on-line. Here performative actions such as the defacing of websites, e-mail bombs and other forms of hacktivism are done on-line.

Tools such as websites, blogs and social media commonly are used in digital activism in Uganda.[15] The use of the internet has led to the proliferation of multiple activist websites in Uganda. Websites such as *Radio Katwe*[16] have been incredibly vocal in their criticism of government policies and in their revelation of corruption. Radio Katwe in particular was notorious for claiming to expose the hidden wealth of the country's first family. International websites, such as the now notorious document archive website *WikiLeaks,*[17] have also been instrumental in exposing government weaknesses and corruption in Uganda.[18] Blogs such as *Uganda Record,*[19] run by the veteran journalist Timothy Kalyegira, have also been involved in digital activism.

Social media such as *Facebook, Twitter, WhatsApp* and *YouTube* have been used by everyday Ugandans in digital activism in different forms. They are a source of information with popular news stories being shared by friends, allowing them to spread faster and have wider coverage than previously was possible.[20] Previously, the most common means of receiving news was the radio which had a limited impact due to high regulation and costs.[21] Today anyone with an

15 Chibita (n 9) 71.

16 www.radiokatwe.com/news.htm was closed down by the government of Uganda in 2006 and replaced by the blog http://katwe.blogspot.ug/ (accessed 27 December 2017).

17 https://wikileaks.org/ (accessed 27 December 2017).

18 'WikiLeaks: Museveni dreaded assassination by Gaddafi' *Africa Review* 8 December 2010, http://www.africareview.com/news/WikiLeaks-say-Museveni-dreaded-assassination-by-Gaddafi/979180-1068646-30gbnkz/index.html# (accessed 20 December 2017; 'Wikileaks: Kabaka's views on Museveni' *New Vision 7* September 2011, http://www.monitor.co.ug/News/National/688334-1231792-a5g989z/index.html (accessed 20 December 2017).

19 www.ugandarecord.co.ug (accessed 28 December 2017).

20 T Kalyegira 'Can newspapers survive in the digital era?' *Daily Monitor* 11 February 2018, http://www.monitor.co.ug/OpEd/Commentary/Can-newspapers-survive-digital-era/689364-4299648-124c0y8z/index.html (accessed 10 March 2018).

21 Y Kalyango 'Political news use and democratic support: A study of Uganda's radio impact' (2009) 16 *Journal of Radio and Audio Media* 200.

internet-enabled telephone will regularly receive news shared or passed on by a friend on a social media platform. Social media has bridged the gap between the political elite and the common man as many can now communicate with individuals in high political office via social media platforms. Many high-profile politicians, including the President, have social media accounts where they communicate with citizens and, unlike traditional media such as radio and television, the people communicate back. In 2014 the President of Uganda, Yoweri Museveni, was rated as Africa's most active president on *Twitter,*[22] while his former ally turned opponent, Amama Mbabazi, was rated 'the most conversational world leader' with 95 per cent of his tweets being responses to followers by Burson-Marsteller's *Twiplomacy* study.[23] Social media have given rise to citizen journalism with citizens taking and sharing informative pictures and videos via these platforms. This result is especially useful in circumstances where objective reporting by the established mainstream media houses is likely to be in question, for example during political protests.[24] Pictures and videos have been especially useful in holding the government accountable for brutality by security agencies. In July 2016 supporters of opposition leader, Dr Kiiza Besigye, were brutally attacked by the police while a number of people recorded videos of the incident on their phones. These were soon uploaded onto *YouTube* and went viral with many shared on *WhatsApp*. As a result 13 of the policemen in the videos were charged with assault.[25] In February 2019 an army general and four of his officers assaulted a traffic officer who had stopped them for breaking the traffic rules. A video recording of the incident went viral on social media and the officers were detained.[26]

An emerging but controversial tool of digital activism is hacktivism. This is the use of non-violent but often illegal digital tools to achieve one's goals.[27] It is not always clear where hacktivism has been carried out as some victims, especially governments and companies that hold sensitive data, such as financial institutions, will go out of their way to hide the fact that it occurred. Often it is the elusive perpetrator who announces the incident and takes credit for it. For a government, a successful hack can be humiliating as it undermines its ability to

22 'Museveni most influential African leader on Twitter' *New Vision* 1 July 2014, https://www.newvision.co.ug/new_vision/news/1342213/museveni-influential-african-leader-twitter (accessed 10 March 2018).

23 'Twiplomacy study 2014' 24 June 2014, http://twiplomacy.com/blog/twiplomacy-study-2014/ (accessed 10 March 2018).

24 Z Tufekci *Twitter and tear gas: The power and fragility of networked protest* (2017) 7.

25 'Police brutality: "Officers on the run", Kayihura summoned' *The Observer* 25 July 2016, http://observer.ug/news-headlines/45538-police-brutality-offending-officers-on-the-run (accessed 22 December 2017).

26 'Kyaligonza will face the law for beating traffic officer – President Museveni' *NTV,* http://www.ntv.co.ug/news/national/Kyaligonza-will-face-the-law-for-beating-traffic/4522324-5014668-12ym9td/index.html (accessed 8 March 2019).

27 NC Hampson 'Hacktivism: A new breed of protest in a networked world' (2012) 35 *Boston College International and Comparative Law Review* 511.

secure data. In May 2010 the Ugandan State House website was hacked into and a conspicuous picture of Adolf Hitler with the swastika, a Nazi party symbol, was posted below that of President Museveni meeting with a Member of Parliament.[28] In August 2012 the hacker collective Anonymous hacked into the Ugandan Office of the Prime Minister's website and left a message protesting against the Anti-Homosexuality Bill.[29] Hacktivism is a controversial tool for digital activism as it inevitably involves breaking local and international laws against hacking.[30]

Even the less obtrusive forms of digital activism in Uganda have attracted the attention of the government. In May 2013 the security minister announced the creation of a social media monitoring centre 'to weed out those who use it to damage the government and people's reputations'.[31] In August 2013 *Facebook* revealed that the government of Uganda was among the 74 countries that had requested information relating to *Facebook* account holders in the first six months of that year.[32] Digital activism in the political sphere is critical as it enables government critics and political activists to broadcast their message without fear of traditional forms of censorship, which target mainstream media houses.[33] When radio and television stations announced that they had been warned by their regulator, the Uganda Communications Commission (UCC), not to host the popular opposition MP, Robert Kyagulanyi, he simply took to his *Facebook* page where he nonchalantly continued sharing his message, posting the following: [34]

28 'Hacker posts Hitler photo on State House website' *Daily Monitor* 31 May 2010, http://www.monitor.co.ug/News/National/688334-929108-brnt54z/index.html (accessed 16 September 2017).

29 CIPESA 'State of internet freedoms In East Africa 2015: Survey on access, privacy and security online' September 2015, http://www.cipesa.org/?wpfb_dl=193 (accessed 3 October 2016).

30 R Solomon 'Criminals or activists? Finding the space for hacktivism in Uganda's legal framework' (2017) 28 *Stellenbosch Law Review* 508.

31 F Emorut 'Government plans to monitor social media' *New Vision* 31 May 2013, https://www.newvision.co.ug/new_vision/news/1321505/gov-plans-monitor-social-media (accessed 8 March 2019).

32 C Stretch 'Global government requests report' Facebook 27 August 2013, https://newsroom.fb.com/news/2013/08/global-government-requests-report/ (accessed 8 March 2019).

33 The censorship of mainstream media houses in Uganda has taken the form of raids and shutdowns. Radio stations have been shut down for airing political controversies. 'UCC closes Kanungu radio for "fuelling public insecurity"' *The Observer* 23 October 2017, https://observer.ug/news/headlines/55557-ucc-closes-kanungu-radio-for-fuelling-public-insecurity (accessed 12 March 2019); television stations have been shut down: 'In Uganda, government shuts down new TV station' *CPJ* 7 February 2007, https://cpj.org/2007/02/in-uganda-government-shuts-down-new-tv-station.php (accessed 10 March 2018); newspaper offices have been raided and shut down: 'Uganda's *Daily Monitor* raided over Museveni "plot"' *BBC News* 20 May 2013, http://www.bbc.com/news/world-africa-22599347 (accessed 10 March 2018).

34 'Bobi Wine speaks out on being banned from TV, radio shows' *The Tower Post* 30 September 2017, http://thetowerpost.com/2017/09/30/bobi-wine-speaks-out-on-being-banned-from-tv-radio-shows/ (accessed 10 March 2018).

> They should also remember that we are in this age of social media. The world is more connected than before. Tell your friend to tell their friend that I shall still communicate to the world through Facebook, Twitter, and our website. If they stop us from going to radio, we shall send out voice notes on WhatsApp. No matter what happens, we shall speak – because we speak for the people. And the voice of the people is the voice of God.

3 Digital activism and freedom of expression

3.1 International law

Article 19 of the Universal Declaration of Human Rights (Universal Declaration)[35] states that everyone has the right to freedom of expression, and this includes the right to 'impart information and ideas through any media'. Since its adoption in 1948, parts of the Universal Declaration, including article 19, have gained wide acceptance and are now regarded as having acquired legal force as customary international law.[36]

Article 19(1) of the International Covenant on Civil and Political Rights (ICCPR)[37] provides that everyone has the right to hold opinions without interference. Article 19(1) is an unqualified right and is not limited by article 19(3), as will be seen. Although freedom of opinion is not listed among the non-derogable rights in article 4, the United Nations (UN) Human Rights Committee (HRC), the treaty-monitoring body for ICCPR, has argued that it in is fact non-derogable as it can never be necessary to derogate from it even in a state of emergency.[38] This argument is relevant to digital activism as the freedom to hold ideas is a *sine qua non* to disseminating them.

Article 19(2) of ICCPR protects freedom of expression.[39] The article's emphasis on 'any other media' as a form of expression certainly covers new innovations in information and communication technologies (ICT).[40] Blocking access to websites has been held to be a violation of the right to freedom of expression enshrined in article 10 of the European Convention on Human Rights (European Convention), which is similar to article 19 of ICCPR.[41] This right, therefore, supports digital activism as it allows for the dissemination of ideas on-line.

---

35 Universal Declaration of Human Rights UNGA Res 217 (III).

36 *Filartiga v Pena-Irala* 630 F 2d 876 (1980) (US Circuit Court of Appeals, 2nd circuit).

37 International Covenant on Civil and Political Rights 999 UNTS 171.

38 General Comment 34 on article 19 of the International Covenant on Civil and Political Rights CCPR/C/GC/34, 102nd session Geneva, 11-29 July 2011 para 5.

39 Article 19: '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.'

40 T Sorell 'Human rights and hacktivism: The cases of Wikileaks and Anonymous' (2015) 7 *Journal of Human Rights Practice* 391.

41 *Yıldırım v Turkey* ECtHR 3111/10 Judgment 18/12/2012.

Article 19(3) of ICCPR sets a three-pronged test for acceptable limitations to freedom of expression under article 19(2). First, the limitation must be provided for by law. This must be a 'national law of general application which is consistent with the Covenant'[42] and must not be 'arbitrary or unreasonable'.[43] Therefore, the law must meet standards of clarity and precision so that people can easily foresee the consequences of their actions in light of it. Second, the law restricting free expression must have a legitimate aim. The list of legitimate aims is not open-ended. They are provided for in article 19(3) of ICCPR, namely, 'respect for the rights and reputations of others, and protection of national security, public order, public health or morals'. They are exclusive and cannot be added to.[44] Finally, any limitation must be absolutely necessary. Even if the limitation is in accordance with a clearly-drafted law and serves a legitimate aim, it must be truly necessary for the protection of the legitimate aim. Any law limiting on-line freedom of expression and, by extension, digital activism must pass muster under these provisions.

In September 2011 the HRC issued General Comment 34[45] in relation to article 19. This is an authoritative interpretation of the minimum standards guaranteed by article 19 of ICCPR. The General Comment emphasises that freedom of expression is necessary for the full development of an individual and constitutes 'the foundation stone for every free and democratic society'. It further notes:

> States parties should take account of the extent to which developments in information and communication technologies, such as internet and mobile-based electronic information dissemination systems, have substantially changed communication practices around the world.

The General Comment emphasises the fact that the legal framework regulating the media should take into consideration the fact that the Internet has created a global network through which ideas and opinions are exchanged without relying on the traditional mass media intermediaries. Finally, the General Comment clarifies the application of article 19(3) which permits restrictions on the right to free expression. Article 19(3) can never justify the restriction of any human rights and democracy advocacy. It can, however, be employed to justify laws that protect respect for the rights or reputations of others and the protection of national security or of public order.[46] Thus, for example, laws restricting the advertising of tobacco-related products, though limiting freedom of expression, have been considered acceptable.[47]

---

42 The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, 28 September 1984, E/CN 4/1985/4 Principle 15.

43 Siracusa Principles (n 42) Principle 16.

44 Siracusa Principles Principle 21.

45 General Comment 34 (n 38).

46 As above.

47 *RJR-MacDonald Inc v Attorney-General of Canada* (1995) 3 LRC 653.

Freedom of expression in these provisions focuses on freedom to disseminate one's views in the public sphere. The public sphere over time has migrated from physical locations to the internet and has expanded, becoming more global in its reach.[48] As an extension of traditional off-line activism to on-line platforms, digital activism deserves the same level of protection as traditional forms of activism. In June 2012 the Human Rights Council unanimously adopted a resolution on the promotion, protection and enjoyment of human rights on the internet.[49] The Council affirmed that '[t]he same rights that people have off-line must also be protected on-line, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice'.

In June 2016 the Human Rights Council adopted a second resolution on the protection of human rights on the internet.[50] This resolution recognised 'the global and open nature of the internet as a driving force in accelerating progress towards development'. The resolution also called upon states to promote digital literacy and to facilitate internet access. The resolution further called upon states to address security concerns regarding the internet to ensure protection of freedom of expression, privacy and other human rights on-line, so that the internet can remain a vibrant force that generates economic, social and cultural development. The resolution unequivocally condemned all human rights violations committed against individuals for exercising their fundamental freedoms on the internet. Finally, the resolution condemned measures that intentionally prevent or disrupt internet access in violation of international human rights law.

3.2 African Charter on Human and Peoples' Rights

Article 9 of the African Charter on Human and Peoples' Rights (African Charter)[51] provides that every individual has the right to receive information and to express and disseminate opinions within the law. In interpreting article 9, the African Commission on Human and Peoples' Rights (African Commission) asserted the 'fundamental importance of freedom of expression and information as an individual human right, as a cornerstone of democracy and as a means of ensuring respect for all human rights and freedoms'.[52] Unfortunately, the full effect of the article appears to be diluted by a claw-back clause

48 T Oladepo 'Digital media activism and Nigeria's public sphere' (2015) 1 *Law, Social Justice and Global Development*, https://warwick.ac.uk/fac/soc/law/elj/lgd/2016-1/tomi_final.pdf (accessed 12 March 2019).

49 UN Human Rights Council Resolution A/HRC/20/L.13, adopted 29 June 2012.

50 UN Human Rights Council, Resolution A/HRC/32/L.20, adopted 27 June 2016.

51 African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) 1520 UNTS 217.

52 *Law Office of Ghazi Suleiman v Sudan II* (2003) AHRLR 144 (ACHPR 2003).

restricting forms of expression to those sanctioned by law.[53] However, the African Commission has found laws restricting freedom of speech to be contrary to article 9.[54] Further, the African Commission has stated before that speech that promotes human rights protection is of special value to society and deserving of protection.[55]

Notably, article 9 includes the right to receive information, which is absent in explicit form in the international human rights instruments discussed above. At the time of their adoption these instruments were not understood to include a right to access information held by public bodies.[56] However, broader interpretations of these international instruments to include the right of access to information have since been adopted.[57] The African Commission in April 2013 adopted the Model Law on Access to Information for Africa. It provides detailed and practical information on the legislative obligations of member states to the African Charter with regard to the right of access to information. The Model Law promotes the establishment of mechanisms to give effect to the right of access to information in a manner which 'enables persons to obtain access to accurate information of information holders as swiftly, inexpensively and effortlessly as is reasonably possible'.[58] The internet is one of the mechanisms which can ensure access to information in a swift and inexpensive manner.

The African Commission in 2002 issued a Declaration of Principles on Freedom of Expression in Africa.[59] This is an amplification of article 9 of the African Charter. In its Preamble the Declaration notes 'the important contribution that can be made to the realisation of the right to freedom of expression by new information and communication technologies'. Principle 1 declares that the right to impart and receive information through any form of communication is an inalienable human right and an essential element of democracy. Principle 2 provides that legal restrictions on freedom of expression must serve a legitimate interest and be necessary in a democratic society. Principle 7 provides that an independent public authority

53 R Gittleman 'The African Charter on Human and Peoples' Rights: A legal analysis' (1982) 22 *Virginia Journal of International Law* 667. Even in *Law Office of Ghazi Suleiman v Sudan II* (n 52) the African Commission emphasised that freedom of expression has to be exercised within the law.

54 *Zimbabwe Lawyers for Human Rights & Associated Newspapers of Zimbabwe v Zimbabwe* (2009) AHRLR 235 (ACHPR 2009).

55 *Law Office of Ghazi Suleiman v Sudan II* (n 52).

56 T Mendel *Freedom of information: A comparative legal survey* (2008) 8.

57 See eg Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression UN Doc E/CN.4/1998/40 28 January 1998 para 14.

58 Sec 3(b) of the Model Law on Access to Information for Africa 2013, http://www.achpr.org/files/instruments/access-information/achpr_instr_model_law_access_to_information_2012_eng.pdf (accessed 12 March 2019).

59 Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights 32nd session 17-23 October 2002, Banjul, The Gambia.

should regulate telecommunication and should be adequately protected against political interference. Principle 12 provides that defamation laws should not hold anyone liable for true statements or reasonably-held opinions regarding public figures, that public figures should tolerate a greater degree of criticism and that sanctions should not inhibit the right to freedom of expression. The principle also states that privacy laws should not inhibit the dissemination of information of public interest. The reference in the Preamble to the contribution of information technologies to freedom of expression accentuates the relevance of the principles in the Declaration to on-line freedom of expression.

In 2016 the African Commission passed Resolution 362 on the Right to Freedom of Information and Expression on the Internet in Africa.[60] This Resolution affirms the 'importance of the internet in advancing human and peoples' rights in Africa, particularly the right to freedom of information and expression'.[61] The Resolution calls upon state parties to respect and take legislative and other measures to guarantee the right to freedom of information and expression through access to internet services. States, therefore, should allow easy access to the internet even when it is used to criticise the government. The Resolution, however, urges citizens to exercise their right to freedom of expression on the internet responsibly. What amounts to 'responsible' use of the internet, however, remains unclear. A narrow interpretation of this term is necessary as persons engaging in on-line activism may on occasion use impolite language to communicate dissatisfaction with the *status quo*.[62]

3.3 African Union Convention on Cyber Security and Personal Data Protection

Article 25(3) of the African Union Convention on Cyber Security and Personal Data Protection,[63] while acknowledging the need for legal measures to curb the growing threats to cyber security, requires that the adopted measures do not infringe on human rights guaranteed under the national constitution and international conventions, particularly the African Charter. Article 25(3) singles out freedom of expression as one of the key rights vulnerable to stringent and overreaching cyber security laws.

60 Resolution on the Right to Freedom of Information and Expression on the Internet in Africa ACHPR/Res 362(LIX) 2016.

61 Resolution (n 60) Preamble.

62 S Rukundo '"My President is a pair of buttocks": The limits of online freedom of expression in Uganda' (2018) 26 *International Journal of Law and Information Technology* 252.

63 African Union Convention on Cyber Security and Personal Data Protection 27 June 2014 (EX CL/846 (XXV)).

3.4 East African Community

According to article 6(d) of the Treaty for the Establishment of the East African Community (EAC Treaty),[64] the promotion and protection of human and peoples' rights in accordance with the provisions of the African Charter is one of the fundamental principles. The East African Court of Justice has held that freedom of expression falls within that article.[65] In today's increasingly digital environment the individual's freedom of expression is most conveniently exercised on-line.

3.5 Ugandan Constitution

Article 29 of the Constitution of Uganda protects freedom of expression in Uganda. Although the Constitution does not define what freedom of expression entails, the Ugandan Supreme Court in *Obbo*[66] defined it as 'freedom to hold opinions and to receive and impart ideas and information without interference'.[67] The Court also noted that the right to freedom of expression was not confined to 'categories, such as correct opinions, sound ideas or truthful information'. The Court stated:[68]

> A person's expression or statement is not precluded from the constitutional protection simply because it is thought by another or others to be false, erroneous, controversial or unpleasant. Everyone is free to express his or her views.

Thus, simply because the mode of expression chosen is impolite or annoying does not justify its suppression. In *Mwenda* sections 39 and 40 of the Penal Code Act, which provided for the crime of sedition, were found to be unconstitutional, the Court noting:[69]

> Our people express their thoughts differently depending on the environment of their birth, upbringing and education. While a child brought up in an elite and God-fearing society may know how to address an elder or leader politely, his counterpart brought up in a slum environment may make annoying and impolite comments, honestly believing that that is how to express him/herself.

The Court noted that the people have a right to criticise their leaders rightly and advised that 'leaders should grow hard skins to bear'.

64 Treaty for the Establishment of the East African Community adopted on 30 November 1999, entered into force 7 July 2000 2144 UNTS 255.

65 *Burundian Journalists' Union v Attorney-General* EACJ Ref 7 of 2013.

66 *Obbo & Another v Attorney-General* [2004] 1 EA 265.

67 As above.

68 As above.

69 *Andrew Mujuni Mwenda & Another v Attorney-General* Constitutional Petition 12 of 2005 para 78.

New forms of technology do not warrant a narrower application of the right to freedom of expression.[70] In *Rwanyarare*[71] the Court considered a provision of the Referendum Act 2002[72] which prohibited the use of electronic media to make false, malicious, sectarian and derogatory statements and also prohibited the use of 'exaggerations or using caricatures' and 'derisive or mudslinging words'. Electronic media was defined as including 'television, radio, internet and email and any other similar medium'. The Court found these provisions unconstitutional as they were far-reaching and draconian and could 'only be intended to intimidate the media contrary to the spirit of article 29(1)(a)'.

According to article 43 a limitation to the right to freedom of expression is acceptable where exercising the right would prejudice the rights of others or prejudice public interest. However, for any such limitation to be acceptable it must be a measure that is accepted and demonstrably justifiable in a free and democratic society.[73] In *Obbo*[74] the Supreme Court noted that the Constitution's primary objective is the protection of the guaranteed rights, including freedom of expression, while limiting their enjoyment is an exception to their protection and, therefore, a secondary objective. Although the Constitution provides for both, the primary objective is dominant and can be overridden only in the exceptional circumstances that give rise to that secondary objective. Even when such limitation occurs, only minimal restraint to the enjoyment of the right, required by the exceptional circumstances, is permissible.[75]

4 Legislation limiting digital activism in Uganda

4.1 Penal Code Act

Section 179 of the Penal Code Act creates the offence of criminal libel. The provision states:

> Any person who, by print, writing, painting, effigy or by any means otherwise than solely by gestures, spoken words or other sounds, unlawfully publishes any defamatory matter concerning another person, with intent to defame that other person, commits the misdemeanour termed libel.

70 X Li 'Hacktivism and the First Amendment: Drawing the line between cyber protests and crime' (2013) 27 *Harvard Journal of Law and Technology* 301; Sorell (n 40).

71 *Rwanyarare v Attorney-General* Constitutional Petition 5 of 1999.

72 The Act had been passed to regulate the referendum in which the people of Uganda would choose to be governed either by the 'Movement system', which was a thinly-veiled one-party system, or the multi-party system.

73 *Obbo* (n 66).

74 As above.

75 As above.

The offence is framed in much the same terms as the civil tort.[76] Although the wording clearly envisages the off-line environment, in *Uganda v Nyakahuma Kalyegira*[77] the Court relied on the definitions of computer output and electronic record in the Computer Misuse Act 2011 (CMA), which included material which can be printed, to find that publication on-line was an offence under section 179. Thus, on-line defamation leaves one liable to prosecution for criminal libel. In considering the limitation that the offence of criminal libel places on freedom of expression, it has been stated that freedom of expression is not a licence to malign others or to repeat unsubstantiated falsehoods. Rather, it is a freedom to be exercised responsibly and with great care so as not to unnecessarily injure the reputations of innocent people.[78] The Ugandan Constitutional Court in *Buwembo*[79] held that section 179 of the Penal Code Act was compatible with freedom of expression guaranteed under the Constitution. The Court reasoned that the importance of free speech had to be weighed against the importance of reputation, and that statements that are defamatory libel, rather than fall under freedom of expression, in fact serve to stifle it as they do not enhance public knowledge and development. Similar provisions have been upheld in other jurisdictions.[80]

However, in today's digital age an offence such as criminal libel inevitably has a chilling effect on freedom of expression. The UN Human Rights Committee in General Comment 34[81] argued that '[s]tates parties should consider the decriminalisation of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty'. Similarly, the African Commission passed a resolution[82] for the repeal of criminal defamation laws. This approach was adopted in the Kenyan case of *Okuta*[83] where the offence of criminal defamation in section 194 of the Kenyan Penal Code was found to be unconstitutional as it infringed the right to freedom of expression. The petitioners in that case were accused of posting defamatory material on a *Facebook* page. Contrary to the Ugandan decision of *Buwembo*, the Court held that the alternative civil remedy was satisfactory and adequate to combat the mischief of defamation. Similarly, in *Konate v Burkina Faso*[84] the African Court on Human and Peoples' Rights (African Court), in declaring a criminal defamation law

76 Secs 180-186 of the Penal Code Act Cap 120.
77 HCT-OO-CR-MC-0001-2013.
78 *Republic v Gachoka & Another* [1999] 1 EA 254.
79 *Joachim Buwembo & Others v Attorney-General* Constitutional Reference 1/2008.
80 *M'membe & Another v The People; M'membe & Others v The People* [1996] 2 LRC 280; *Bernard Sullivan v Attorney-General Seychelles* SCA 25 of 2012.
81 United Nations Human Rights Committee (n 45).
82 169: Resolution on Repealing Criminal Defamation Laws in Africa, http://www.achpr.org/sessions/48th/resolutions/169/ (accessed 29 November 2017).
83 *Okuta & Another v Attorney-General & Others* Constitutional Petition 397 of 2016.
84 *Konate v Burkina Faso* African Court of Human Rights App 4/2013.

incompatible with freedom of expression, stated that freedom of expression could be infringed only if that restriction was based on an overarching public interest. The Court stated that criminal defamation laws should be used only as a last resort and only to protect against a serious threat to the enjoyment of other human rights, for instance in cases of hate speech and incitement. Similar reasoning was applied in the Zimbabwean cases of *Madanhire v Attorney-General*[85] and *MISA-Zimbabwe v Minister of Justice,*[86] where it was held that criminal defamation laws were unconstitutional as they were not proportionate to the offence.

4.2 Computer Misuse Act 2011

4.2.1 Cyber harassment

Section 24 of the Computer Misuse Act (CMA) creates the offence of cyber harassment, which is the use of a computer in making obscene requests or threatening to inflict injury to any person or property. The anonymity and ease of communication provided by the internet make cyberspace the ideal roaming ground for people who wish to harass others.[87] The modes of communication available to facilitate cyber harassment include e-mail, blogs, chat rooms, instant messaging services, electronic bulletin boards, and social networking sites.[88]

4.2.2 Offensive communication

Section 25 of the CMA prohibits the wilful and repeated use of electronic communication to disturb the peace, quiet or right to privacy of any person without purpose of legitimate communication. This provision is rooted in the right to privacy guaranteed under the Constitution.[89] The test for offensiveness of communication is that it must disturb the peace, quiet or right to privacy of the recipient, must be done repeatedly and must not be legitimate communication. The requirement that the communication disturbs the peace of another is a subjective one, and what may disturb the peace of individuals may vary from one person to another. The requirement that the communication be done repeatedly means that once-off communications, no matter how disturbing, may not meet the threshold to fall under this section. They may, however, fall under

85 Judgment CCZ 2/14; Zimbabwe Const Application CCZ 78/12.

86 Zimbabwe Const Application CCZ/07/15.

87 D Harvey *Cyberstalking and internet harassment: What the law can do* Australian Institute of Criminology, Netsafe.Org.Nz 2 (2003), http://www.netsafe.org.nz/Doc_Library/netsafepapers_davidharvey_cyberstalking.pdf (accessed 7 February 2018).

88 S Jameson 'Cyber harassment: Striking a balance between free speech and privacy' (2008) 17 *CommLaw Conspectus* 231.

89 Art 27 Constitution of the Republic of Uganda 1995.

cyber harassment.[90] Finally, there must be no legitimate purpose to the communication, meaning that the offender should have no justifiable reason for sending the communication.

There is little doubt that some form of legislation to protect against on-line harassment and abuse is necessary. However, the provisions on cyber harassment and offensive communication as they stand now are particularly prone to abuse by government authorities to restrict on-line criticism. The CMA provisions have been applied in a number of instances. In December 2016 Swaibu Nsamba Gwogyolonga, a political activist, was arrested and charged with offensive communication contrary to section 25 of the CMA after he had posted on his *Facebook* page a photo-shopped picture of the President dead and lying in a coffin, stating that he would announce and mourn the death of the President when he dies.[91] Stella Nyanzi, a Makerere University lecturer with a considerable social media following and a reputation for tincturing her incisive socio-political analyses with sexual allegory, in early 2017 fell victim to a charge of offensive communication following a caustic *Facebook* post in which she called the President 'a pair of buttocks' and the first lady, who is also the Minister of Education, 'empty-brained'. Her post was a complaint against the President and the first lady reneging on their campaign promise to deliver free sanitary towels to girls in school.[92] She is being prosecuted for offensive communication and cyber harassment contrary to the CMA. Unsuccessful attempts were even made to have her dismissed from her employment as a lecturer at Makerere University as a result of her posts.[93] In December 2017 David Mugema and Jonah Muwanguzi were arrested and charged with offensive communication for having electronically communicated through social media a song titled 'Wumula', the lyrics of which called for the resignation of Yoweri Kaguta Museveni, the President of Uganda.[94]

90 Sec 24 Computer Misuse Act 2011.

91 As above.

92 'Fury over arrest of academic who called Uganda's President a pair of buttocks' *The Guardian* 13 April 2017, https://www.theguardian.com/global-development/2017/apr/13/stella-nyanzi-fury-arrest-uganda-president-a-pair-of-buttocks-yoweri-museveni-cyber-harassment (accessed 14 December 2017).

93 'Dr Stella Nyanzi suspended from Makerere University job for insulting Janet Museveni' *NTV* 31 March 2017, http://www.ntv.co.ug/news/local/31/mar/2017/dr-stella-nyanzi-suspended-makerere-university-job-insulting-janet-museveni#sthash.lbtl7UNW.dpbs (accessed 14 December 2017); 'Makerere University ordered to hear Dr Stella Nyanzi disciplinary case afresh' *Daily Monitor* 21 October 2017, http://www.monitor.co.ug/News/National/Makerere-University-ordered-Dr-Stella-Nyanzi-disciplinary-case/688334-4149572-2bugkj/index.html (accessed 14 December 2017).

94 'Court grants bail to artists who annoyed Museveni' *Daily Monitor* 6 December 2017, http://www.monitor.co.ug/News/National/Court-grants-bail-artists-Museveni-Kamasanyu/688334-4217338-ufcw1mz/index.html (accessed 15 December 2017).

4.2.3 Constitutionality of the crimes of cyber harassment and offensive communication

The wording of the provisions of the Computer Misuse Act certainly is prone to attack. Words such as 'obscene', 'lewd', 'lascivious', 'indecent' and 'disturb the peace, quiet' contained in those provisions are not defined in the Act. It may be argued that this makes the offences unclear contrary to article 28(12), which requires that offences be clearly defined. In the Kenyan case of *Andare v Attorney-General*[95] the petitioner argued that section 29 of the Kenya Information and Communication Act, Cap 411A, which provided that a person who sends a grossly offensive or indecent, obscene or menacing message by means of a telecommunications system for the purpose of causing annoyance, inconvenience or needless anxiety to another person, commits an offence. He argued that section 29 of the Act was vague and over-broad, especially with regard to the meaning of 'grossly offensive', 'indecent', 'obscene 'menacing', 'causing annoyance', 'inconvenience' or 'needless anxiety', thereby offending the principle of legality which requires that a law be clear and precise. The Court held that as the Act did not define the words used, the meaning of those words was left to the subjective interpretation of each judicial officer seized of a matter. The law, therefore, was vague, broad and uncertain. In *Rwanyarare*[96] the Court considered a provision of the Referendum Act 2002[97] which prohibited any person from using electronic media to make statements containing words which are 'malicious', 'sectarian', 'abusive or insulting', 'exaggerations or using caricatures' or 'derisive or mudslinging'. The Court found this provision unconstitutional due to vagueness and the fact that if applied, it would only be applied against the opposition side and not the party in power.

The use of these provisions of the CMA to restrict political criticism unconstitutionally limits the freedom of expression guaranteed in the Constitution and international instruments. As noted above, the Ugandan Constitutional Court in *Mwenda*[98] and the African Commission in its Declaration of Principles on Freedom of Expression in Africa[99] stated that public figures should be required to tolerate a greater degree of criticism. This is especially crucial in the case of political figures as freedom of expression is based on the assumption that political leaders are fallible and, therefore, should be open to criticism.[100] As noted in the cases cited above, the CMA provisions

95 Constitutional Petition 149 of 2015.

96 *Dr James Rwanyarare & Another v Attorney-General* Constitutional Petition 5 of 1999.

97 n 72.

98 *Mwenda v Attorney-General* Constitutional Petition 12 of 2005.

99 Declaration of Principles (n 59).

100 C Anthonissen 'The sounds of silence in the media: Censorship and self-censorship' in R Wodak & V Koller *Handbook of communication in the public sphere* (2008) 407.

have been put to prolific use by powerful political figures to control criticism. This use of legislative provisions effectively communicates the state's ability and power to reach into the digital sphere and punish dissent therein. This inevitably has a chilling effect on on-line freedom of expression. In the Kenyan case of *Robert Alai v Attorney-General*[101] Robert Alai, a prominent social media personality and blogger, had posted on Twitter regarding President Uhuru of Kenya that '[i]nsulting Raila is what Uhuru can do. He hasn't realised the value of the Presidency. Adolescent President. This seat needs maturity.' He was charged with undermining the authority of a public official under section 132 of the Kenyan Penal Code. He sought a declaration that section 132 was unconstitutional. The Court, relying on article 33 of the Kenyan Constitution which guarantees freedom of expression, noted that people 'cannot be freely expressing themselves if they do not criticise or comment about their leaders and public officers'. The Court further stated:[102]

> The section does not define the words 'undermining authority of a public officer' leaving it to the subjective view of the person said to have been undermined and/or the court. In a democratic state, constructive criticism of public or state officers is the hallmark of democracy and the means for public accountability. Criminalising criticism is not in accord with a transformative constitution, since senior public officers should routinely be open to criticism. Dissent in opinion should not amount to a crime otherwise this is in effect, suppressing the right to hold different opinion from those in public office.

Thus, laws such as the CMA provisions on cyber-harassment and offensive communication, which lend themselves well to the government as tools of suppression of dissent by restricting criticism of public figures, are of doubtful constitutionality.

4.3 Anti-Terrorism Act 2002

Section 7(2)(g) of the Anti-Terrorism Act (ATA)[103] makes serious interference with or disruption of an electronic system part of the offence of terrorism which on conviction carries the death penalty. The maximum sentence for any of the various forms of hacking criminalised under the CMA is 15 years' imprisonment.[104] The actions that would fall under the CMA provisions would also presumably fall under the ATA provisions. Moreover, the Act does not define 'serious interference' with an electronic system. Any kind of hacking could easily fall into this category. As the same criminal actions could fall under either Act, it is likely that the ATA provision can be used where the hacking takes a political hue in the form of hacktivism. The threat of the death penalty certainly is a considerably stronger disincentive than 10 to 15 years' imprisonment. While hacktivism might be a more

101 Constitutional and Human Rights Division Petition 174 of 2016.
102 Petition (n 101) para 35.
103 Anti-Terrorism Act 2002.
104 Secs 12-15 Computer Misuse Act 2011.

controversial form of digital activism, it does not warrant the death penalty. Moreover, a comparison of the two provisions in the CMA and ATA reveals that while the CMA offence, which carries the 10 to 15 year penalty, is elaborately defined, the ATA offence, which carries the death penalty, is brief and considerably vague.

Part VII of the ATA provides for the legal interception of communication, including data communication, in the investigation of terrorist activities. The Minister of Internal Affairs is empowered to designate for a period of 90 days any member of the Uganda Peoples' Defence Forces, the Ugandan police force or a government security organisation as an authorised officer.[105] An authorised officer is allowed to intercept the communications of any person for purposes of safeguarding public interest and preventing terrorism.[106] The ATA allows 'telephone calls, faxes, emails and other communications'[107] to be intercepted on suspicion of terrorism. The power of surveillance on suspicion of terrorism thus lies squarely in the hands of the executive branch as there is no requirement of authorisation by a judicial officer. Left unchecked, this implies that the threat of legalised surveillance looms over all who attempt to engage in digital activism in Uganda. By law 'telephone calls, faxes, emails and other communications'[108] can be intercepted on suspicion of terrorism.

4.4 Regulation of Interception of Communications Act

Authorisation for the interception of communication can be given under section 2(2) of the Regulation of Interception of Communications Act (RICA),[109] which allows for the *bona fide* interception of a communication in connection with the provision, installation, maintenance or repair of a telecommunication service. Internet service providers are required to ensure that their telecommunication systems are technically capable of supporting lawful interception, undetectable by the target, at all times.[110] Section 5 of RICA requires intelligence agencies and the police to seek judicial authorisation prior to the interception of communications and must demonstrate only 'reasonable' grounds for broad threats to national security, national economic interests and public safety. Information obtained in excess of what the warrant caters for remains admissible at the discretion of the court under section 7. This provision, which allows for illegally-collected evidence, runs contrary to the principles established that where human rights have been violated in the collection of evidence it will not be admitted.[111] Section 10 requires

105 Sec 18 Anti-Terrorism Act.
106 Sec 19 Anti-Terrorism Act.
107 Sec 19(5)(b) Anti-Terrorism Act.
108 As above.
109 Regulation of Interception of Communications Act 18 of 2010 (RICA).
110 Sec 8 RICA.
111 *Besigye v Attorney-General* Constitutional Petition 7 of 2007; *Uganda v Sekabira* [2012] UGHC 92. However, see *Maycock v Attorney-General* [2010] 3 LRC 1.

that a person in possession of a decryption key where the data collected by interception is encrypted must use it to disclose the encrypted information upon request by the authorised person.

Section 11 requires internet service providers to retain metadata but does not specify the terms and conditions of the retention. This provision is likely to be in conflict with the Data Protection and Privacy Act, which allows for the data subject to request for data in relation to him or her to be erased.[112] RICA does not provide a right to seek redress for individuals that are the subject of a warrant for interception of communication. Thus, if an individual discovers that he or she is under surveillance, the only remedy is a court process which can be lengthy and expensive. The Act also fails to provide a right to notification following an investigation to inform an individual that they had been subjected to communication surveillance. Instead, section 15 places a gag on internet service providers and their employees, preventing them from even revealing statistics and other relevant information on the number and nature of communication interception requests received which hinders transparency,[113] and is contrary to the Data Protection and Privacy Act, which allows the data subject to be informed of any data being processed.[114]

Internet service providers have access to a broad range of sensitive information and data relating to their subscribers, such as metadata, the content of their communications, location, and so forth.[115] Where the government is able to access this information from internet service providers, it likely will hamper digital activism. The state can use this information acquired through surveillance to identify dissidents, anticipate planned dissent and signal its power to the masses, discouraging them from engaging in on-line activism.[116] It is undeniable that under certain circumstances there might be legitimate reasons to intercept communication. In the Indian case of *People's Union for Civil Liberties v Union of India*[117] the Indian Telegraph Act 1885 allowed for the interception of telegraph messages in the event of a public emergency or in the interests of public safety if it was necessary or expedient to do so. A report on 'Tapping of politicians' phones' highlighted several deficiencies in the way in which the law had in practice been applied, such as that interception had continued beyond authorised periods (albeit in certain cases in good faith on oral requests) and that various authorised agencies were

112 Sec 24 of the Data Protection and Privacy Bill 2015.

113 The issuing of 'transparency reports' by internet service providers in which they disclose the requests for information and surveillance received from governments has been acknowledged as one of the mechanisms of maintaining freedom of expression. R MacKinnon et al *Fostering freedom online: The role of internet intermediaries* (2014) 3.

114 Sec 24 Data Protection and Privacy Act 2019.

115 MacKinnon (n 113) 80.

116 AR Gohdes *Repression in the digital age: Communication technology and the politics of state violence* (2014) 28.

117 [1999] 2 LRC 1 (India).

not maintaining files regarding the interception of telephones. The constitutionality of the law providing for interception was challenged. The Court held that the substantive law in the Indian Telegraph Act 1885, setting out the conditions under which the power to order the interception of messages could be exercised, required procedural backing in order to ensure that the exercise of such power was fair and reasonable. In this instance, such procedure had not been laid out. However, the Court noted that where the interception of communication by state authorities is established under procedure by law which prevents the arbitrary exercise of such power, this would not violate the right to privacy or freedom of expression. However, with RICA the challenge is that it is likely that this law will be abused and used by the government to spy on political opponents rather than potential criminals. As was noted in *Rwanyarare*, a law might appear neutral but, given the legal-political realities of the day, is likely to be used against government opponents. In such a scenario, such a law should not be allowed to stand.

4.5 Anti-Pornography Act 2014

The Anti-Pornography Act prohibits the production, trafficking, publishing and broadcasting of pornography.[118] The Act also established the Pornography Control Committee[119] which is empowered, among others, to 'ensure the early detection and prohibition of pornography'.[120] While the government's war on pornography is ostensibly touted as a moral crusade to reclaim the minds of Uganda's youth, it has implications beyond morality. In August 2017 the Minister of Ethics and Integrity announced that Uganda would soon be acquiring a 'pornography-detecting machine'.[121] The machine, purchased at the cost of US $88 000, was said to be able to detect deleted or current pornographic materials stored on people's computers. The Minister, in an impassioned speech, fulminated against pornography, which he claimed was 'one of the deadliest moral diseases in this country' contributing to 'escalating cases of drug abuse among youths, incest, teenage pregnancy and abortion, homosexuality and lesbianism and defilement'.[122] While some commentators easily dismissed the idea of a pornography-detecting machine as laughable,[123] others noted with suspicion that it was part of a general trend towards greater

118 Sec 13 Anti-Pornography Act 2014.

119 Sec 3 Anti-Pornography Act 2014.

120 Sec 7 Anti-Pornography Act 2014.

121 'Porn detector machine to arrive soon – Minister Lokodo' *The Observer* 28 August 2017, http://observer.ug/news/headlines/54639-porn-detector-machine-to-arrive-soon-minister-lokodo.html (accessed 16 December 2017).

122 As above.

123 'Uganda buys a "pornography detection machine" to catch offenders, official says' *The Huffington Post* 8 February 2016, https://www.huffingtonpost.com/entry/uganda-pornography-detection-machine_us_57a102c7e4b08a8e8b5fe897 (accessed 16 December 2017).

surveillance.[124] The purpose of this machine is 'to monitor and or intercept, downloading, watching, sharing and or transmission of electronic pornographic material'.[125] This suggests that the ridiculous-sounding 'pornography detecting machine' may in fact be a more sinister form of Deep Packet Inspection (DPI) technologies[126] that will enable the government to conduct effective surveillance. DPI is a popular form of monitoring for child pornography worldwide and all forms of pornography in countries with stringent obscenity laws. However, it has been noted that while the initial target ostensibly may be pornography, many governments subsequently use these technologies to spy on their citizens.[127] Russia, China and Iran are countries that are noted to have used DPI with considerable success in on-line surveillance and to control the content that their citizens can access.[128]

4.6 Uganda Communications Act 2013

The Uganda Communications Act 2013[129] establishes the Uganda Communications Commission (UCC) and empowers it 'to monitor, inspect, license, supervise, control and regulate communications services'.[130] The Minister of Information and Communication Technologies appoints all members of the Board that governs the UCC.[131] This places the Commission firmly under the control of the executive branch of government and makes it amenable to its influence. This practice is contrary to Principle 7 of the Declaration of Principles on Freedom of Expression in Africa which requires a public authority regulating the telecommunications sector to be independent. The Act in section 86 also empowers the UCC to 'direct any operator to operate a network in a specified manner in order to alleviate the state of emergency'. Under the Constitution it is the President who declares a state of emergency.

124 'Uganda's "pornography-blocking machine" appears to be part of a darker censorship agenda' *iAfrikan* 26 August 2016, https://www.iafrikan.com/2016/08/26/ugandas-pornography-blocking-machine-appears-to-be-part-of-a-darker-censorship-agenda/ (accessed 16 December 2017).

125 'Lokodo appoints committee to fight pornography' *Daily Monitor* 29 August 2017, http://www.monitor.co.ug/News/National/Lokodo-appoints-committee-to-fight-pornography/688334-4074914-m7iysl/index.html (accessed 16 December 2017).

126 This is software that examines a data packet as it passes an inspection point, searching for any defined criteria to decide whether the packet may pass or whether it needs to be routed to a different destination.

127 S Stalla-Bourdillon, E Papadaki & T Chown 'From porn to cybersecurity passing by copyright: How mass surveillance technologies are gaining legitimacy: The case of deep packet inspection technologies' (2014) 30 *Computer Law and Security Review* 670.

128 C Fuchs 'Implications of deep packet inspection (DPI) internet surveillance for society' July 2012 The Privacy and Security Research Paper Series, http://fuchs.uti.at/wp-content/uploads/DPI.pdf (accessed 16 December 2017).

129 Sec 4 Uganda Communications Act 2013.

130 As above.

131 Sec 9(3) Uganda Communications Act 2013.

The UCC has generally functioned as another arm of the ruling party taking action against media houses and, through telecommunications companies, against the internet whenever it has been in the government's interests.[132] In that respect, it has frequently taken blatantly unconstitutional actions to aid the government.

4.6.1 Shutting down of websites critical of the government by the Uganda Communications Commission

The UCC has ordered the shutdown of private websites critical of the government. The Commission appears to order the shutdown of websites on the basis of its general powers of regulation as there is no specific provision in the Communications Act that confers that authority. Websites are stored on servers, which have internet protocol (IP) addresses. All the government has to do is have the UCC order internet service providers and telecommunication companies to block access to a specific IP address.[133] In the run-up to the presidential elections of 2006 the Ugandan government through the UCC ordered MTN, at the time the country's main internet service provider, to block internal access to a critical website called *Radio Katwe.*[134] MTN issued a statement explaining that it decided to comply as Ugandan law 'empowers [UCC] to direct any telecoms operator to operate networks in such a manner that is appropriate to national and public interest'.[135] *Radio Katwe* was notorious for publishing reports that were extremely critical of the President, his family and the ruling party,[136] claiming that the goal was to 'campaign for the end of dictatorship, corruption, persecution, poverty … in Uganda'.[137] The site claimed to have been receiving up to 71 000 hits in one day.[138] In February 2006 the government blocked access to the website of the *Daily Monitor*, a privately-owned daily newspaper, because it was publishing election results without the authorisation of the Electoral Commission. The blockage was

132 PG Mwesigye 'UCC deserves more attention from media, civil society, and Parliament' *ACME* 29 November 2017, https://acme-ug.org/2017/11/29/ucc-deserves-more-attention-from-media-civil-society-and-parliament/ (accessed 13 March 2018).

133 'How African governments block social media' *BBC News* 25 April 2016, http://www.bbc.com/news/world-africa-36024501 (accessed 16 December 2017).

134 'Critical website Radio Katwe blocked on eve of presidential election' *Open Net Africa* 22 February 2006, http://www.opennetafrica.org/critical-website-radio-katwe-blocked-on-eve-of-presidential-election/ (accessed 12 December 2017); 'UCC ordered blocking Radio Katwe MTN' *New Vision* 20 February 2006, http://www.newvision.co.ug/new_vision/news/1154037/ucc-blocking-radio-katwe-eur-mtn (accessed 13 December 2017).

135 *Open Net Africa* (n 134).

136 'Museveni's family ownership of Uganda' *Radio Katwe* 13 May 2015, http://radiokatwenews2013.blogspot.ug/2015/05/musevenis-family-ownership-of-uganda.html (accessed 12 December 2017).

137 http://radiokatwenews2013.blogspot.ug/ (accessed 12 December 2017).

138 *Open Net Africa* (n 134).

removed only after the Electoral Commission had declared the official results.[139] The *Daily Monitor* had aimed at declaring results from the different polling stations so that they could be compared to those of the Electoral Commission. The official results of the election subsequently were unsuccessfully contested in *Besigye v Electoral Commission.*[140] In the same period it was reported that the website of the state-owned newspaper, *New Vision*, also had been blocked.[141]

Like many other African governments, the Ugandan government on occasion has cracked down on social media. On 18 February, the day of the 2016 presidential elections, the President ordered the blocking of access to social media platforms such as *Facebook*, Twitter and *WhatsApp*. According to the President, the move was prompted by fears of widespread panic among the masses as a result of disinformation spreading.[142] In his own words, the President asserted that he would not tolerate 'people telling lies using social media. Don't joke with the state. It can do more if people keep misbehaving.'[143] However, despite this threatening stance, many people gained access to the social media sites via virtual private network (VPN) applications during the period of the shutdown. VPNs redirect the user's internet activity to a computer in a different country where the blocks have not been imposed. One opposition presidential candidate went so far as to guide people on how to access the VPNs on his social media page.[144] On 12 May 2016, the date of the swearing in of President Museveni for a fifth elective term, internet service providers in Uganda were once again ordered by the UCC to block access to *Facebook*, *WhatsApp* and *Twitter*. According to the UCC the orders had come from state security organs, which cited 'security reasons' for the shutdown.[145] In *Legal Brains Trust Ltd v UCC*[146] a constitutional petition was brought to declare that the shutting down of social media platforms during the election period was unconstitutional. However, the Court dismissed the case arguing

139 Chibita (n 9) 69.

140 *Rtd Col Dr Kizza Besigye v Electoral Commission, Yoweri Kaguta Museveni* [2007] UGSC 24.

141 'Government blocks *New Vision*, *Daily Monitor* websites ahead of election' *Radio Katwe* 20 February 2006, http://katwe.blogspot.ug/2006/02/government-blocks-new-vision-daily.html (accessed 16 December 2017).

142 'Uganda election: Facebook and WhatsApp blocked' *BBC News* 18 February 2016, http://www.bbc.com/news/world-africa-35601220 (accessed 13 December 2017).

143 'Museveni endorses Besigye arrest; threatens tighter social media controls' *Chimp Reports* 21 February 2016, http://www.chimpreports.com/museveni-endorses-besigye-arrest-threatens-tighter-social-media-controls/ (accessed 13 December 2017).

144 *BBC News* (n 142).

145 'Government shuts down social media again' *Daily Monitor* 13 May 2016, http://www.monitor.co.ug/News/National/Government-shuts-down-social-media-again/688334-3201024-qxvhrxz/index.html (accessed 16 December 2017).

146 HCMC 16 of 2016.

that the petitioner had not exhausted other remedies such as the tribunal that deals with telecommunications sector issues.[147]

The shutting down of these websites, especially the social media websites, is a severe limitation on digital activism in the country. Shutting down websites that are critical of the government discourages the creation of such websites, which are necessary to hold the government to account. It also denies those who set up these websites their right to disseminate their views and opinions. Shutting down social media is even more frustrating to digital activists. Social media functions as a tool for citizens to provide feedback to government. Ninety per cent of ministries, departments and agencies in Uganda use social media to obtain and respond to citizens' opinions, reviews and questions.[148] Citizen feedback to government acts as a check on bureaucratic abuse and corruption, alerts the government to citizens' needs and concerns, and gives citizens a sense that they have a voice in society.[149]

4.7 Excise Duty (Amendment) Act 2018

In March 2018 the Ugandan government proposed the introduction of a tax on social media. The idea was initiated by the President of Uganda, Mr Yoweri Museveni, who argued that Ugandans were using social media platforms for *lugambo* (gossip), and that the tax was meant to 'raise resources to cope with the consequences of their *lugambo*'.[150] In May 2018 the Excise Duty (Amendment) Act 2018 was passed. This Act introduced the taxation of social media platforms which it referred to as 'over the top services' (OTT). The Act defines OTT as 'transmission or receipt of voice or messages over the internet protocol network and includes access to virtual private networks'.[151] A tax rate of UGX 200 (US $0,06) is imposed on each OTT service user for 24 hour access.[152] The internet service provider is liable to account for and pay the excise duty.[153]

The tax hinders digital activism as it discourages the use of social media. Social media largely functions as a gateway to information and communications technology and greater internet use, and is the most

147 Similarly, in *ZLHR and MISA Zimbabwe v Minister of State for National Security* Case HC 265/19 the petition against the constitutionality of a social media shutdown was concluded on a technical point without examining freedom of expression.

148 NITA-U, National Information Technology Survey 2017/18 Report 158 (March 2018).

149 M Warschauer *Technology and social inclusion: Rethinking the digital divide* (2003) 177.

150 'President Museveni apparently proposes taxing social media' *Techjaja* 31 March 2018, https://www.techjaja.com/president-museveni-apparently-proposes-taxing-social-media/ (accessed 12 March 2019).

151 Sec 2 Excise Duty (Amendment) Act 2018.

152 Sec 6(e) Excise Duty (Amendment) Act 2018.

153 Sec 3 Excise Duty (Amendment) Act 2018.

common use of the internet in Uganda.[154] In June 2018, a month before the introduction of the tax, the internet penetration rate in Uganda stood at 47,4 per cent (18,5 million internet users). By September, a mere three months later, it had fallen to 35 per cent (13,5 million users).[155] The decrease in the number of internet users reduces the efficacy of digital activism.

5 Conclusion

Digital activism has the nature of social and political activism, making these more widespread and easier. International instruments and constitutions protect freedom of expression and, by extension, digital activism. This protection notwithstanding, various laws are being applied to curtail digital activism. A balanced approach that acknowledges the value of digital activism yet curtails harmful aspects of information and communications technology, such as cybercrime, is needed so that freedom of expression, so critical in this digital age, can thrive.

154 UCC 'Access and usage of communication services across Uganda' January 2015, http://ucc.co.ug/files/downloads/20150130-UCC-access-usage-dissemination.pdf (accessed 12 March 2019).

155 J Nanfuka 'Social media tax cuts Ugandan internet users by five million, penetration down from 47% to 35%' *CIPESA* 31 January 2019, https://cipesa.org/2019/01/%EF%BB%BFsocial-media-tax-cuts-ugandan-internet-users-by-five-million-penetration-down-from-47-to-35/ (accessed 12 March 2019).