JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
eISSN: 2788-6727 — Volume 1, Issue 1 (2021) pp. 91-114.
https://doi.org/ 10.52907/jipit.v1i1.67

Appraising the Impact of Kenya's Cyber-Harassment Law on the Freedom of Expression

Abdulmalik Sugow[*]
Margaret Zalo[**]
Isaac Rutenberg[***]

ABSTRACT

Kenya's Computer Misuse and Cybercrimes Act makes it an offence, in Section 27, for a person to communicate with another a message that they know or ought to know would cause the recipient fear; is indecent or offensive in nature; or would detrimentally affect the recipient. This offence carries a penalty of either a 20 million shilling fine or a 10-year term of imprisonment or—discretionarily—both. While the offence is termed 'cyber-harassment', its wording appears to exclude a number of offences that would count as cyber-harassment such as cyber-stalking, doxing or impersonation. In fact, its wording is vague and

[*] The author holds an LLB from Strathmore University (Nairobi, Kenya).

[*] The author holds an LLB from Strathmore University (Nairobi, Kenya).

[*] The author is a senior lecturer at Strathmore University (Nairobi, Kenya) and holds a BSc. in Chemistry and Mathematics(Computer Science at Colorado School of Mines), a PhD in Chemistry at California Institute of Technology (United States) and JD at Santa Clara University School of Law (California, United States).

overbroad, using undefined terms such as 'detrimentally affect' which require subjective interpretation. Cyber-harassment laws constitute a limitation on the freedom of expression and as such, ought to conform to the limitations of human rights test as provided in Article 24 of the Constitution. Where the aim sought is legitimate in a democratic society and other conditions such as legality are met, this limitation is valid. This paper reviews Kenya's law that was recently upheld by the High Court in Bloggers Association of Kenya (BAKE) v Attorney General & Three others; Article 19 East Africa & another and finds that it fails to meet the limitations test prescribed under Article 24 of the Constitution. It argues that Section 27 of the Computer Misuse and Cybercrimes Act is therefore overbroad and has the potential to be used as a tool for the unconstitutional suppression of legitimate criticism.

Keywords: Africa, Cyber-Harassment, Freedom of Expression, Overbreadth Doctrine, Political Speech

TABLE OF CONTENTS

1. INTRODUCTION

In 2018, Kenya enacted the Computer Misuse and Cybercrimes Act (the CMCA). Shortly after its enactment, its constitutionality was challenged at the High Court in *Bloggers Association of Kenya (BAKE) v. Attorney General & 5 others* (2018). Among the challenged provisions was Section 27 which provides for the offence of cyber-harassment. It reads as follows:

> 27. (1) A person who, individually or with other persons, willfully communicates, either directly or indirectly, with another person or anyone known to that person, commits an offence, if they know or ought to know that their conduct—
>
> (a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that person's property; or
>
> (b) detrimentally affects that person; or
>
> (c) is in whole or part, of an indecent or grossly offensive nature and affects the person.

According to BAKE's petition, the problem with this offence lied in its broad wording, and the negative effect it could have on the freedom of expression. In the initial stages of parliamentary debate, an international civil society organisation raised the same concern with the wording of the offence. In particular, they argued that the law's vagueness would likely result in its use as a tool by the Government to suppress legitimate criticism (Article19, 2018, p. 16). This was also recognised by a Member of Parliament (MP):

> In its current form, unless properly defined, it could include anything including legitimate criticism. If somebody contacts you continuously, which could be two or three times, then that could amount to cyber-bullying. I do not even know how your constituents who call you twice or three times will contact you because they will be committing a criminal offence. Unless properly redefined, Clause 16 is dangerous (National Assembly Hansard, 2018 March 21, afternoon sitting, p. 23).[1]

[1] The wording of the offence in the Bill included a repetition component and slightly varies from the wording adopted in the final Act. *See* the discussion in Section II for a detailed analysis.

Another MP also noted that in wording the offence broadly, some types of harassment, such as identity theft and unlawful disclosure (doxing), were not captured adequately (*ibid.*, p. 20).

Undisputedly, the oft-cited objective of cyber-harassment law—deterrence of online harassment—is valid in light of the pervasive nature of cyber-space, and the effects of online harassment on people (Laer, 2014, p. 85; National Assembly Hansard, 2018 March 21, afternoon sitting). However, a common problem that arises with laws intended to address this social conduct is their scope. With these laws amounting to a limit on the constitutionally guaranteed freedom of expression, ambiguity in wording may result in the limitation being overbroad and therefore unconstitutional. With the use of subjective language such as "detrimentally affects that person", the CMCA can be described as overbroad. A law is overbroad when, at face value, it limits both protected and unprotected constitutional activity such as free speech (*Grayned v. City of Rockford*, 1972). Since the commission of the offence in the CMCA is contingent upon the subjective perception of communication by the recipient, there lacks an objective standard through which one can predict liability. Such laws run the risk of having a chilling effect on the freedom in question (*Geoffrey Andare v. AG*, 2016). Limits on fundamental freedoms ought to be prescribed by law, in pursuit of a legitimate aim, and should not jeopardise the enjoyment of the freedom in question or other rights (Constitution of Kenya 2010, a. 24 (1)).

The CMCA is not the first instance of an ambiguously worded limit on the freedom of expression in Kenya. Previously, the High Court invalidated Section 29 of the Kenya Information and Communication Act (KICA) a law markedly similar to Section 27 of the CMCA on grounds of its ambiguity. Section 29 of KICA criminalised the 'improper use of a licensed communications system' (Geoffrey Andare v AG, 2016). Shortly after its passage, Section 29 was used to charge a blogger for comments made about public officials. Despite the similarities between KICA and the

CMCA, and the potential that Section 27 of the CMCA would be used in a similar manner, the High Court of Kenya dismissed BAKE's petition (*BAKE v. Attorney General*, 2020).

Perhaps in recognition of the insufficiency of the existing laws to deal with online conduct, a number of African countries have adopted similar approaches to Kenya's legislating for cyber-crime. By 2016, according to the AU, around 11 African countries had laws relating to cyber-crime, with an additional 12 countries having partial provisions in place (African Union Commission, 2016, p. 53; Kshetri, 2019, p. 78). However, this has since changed with the awareness raised by the AU Convention on Cyber Security and Personal Data (2014). Of the countries that have cyber-specific laws, cyber-harassment features distinctly as an offence in Botswana, Kenya, Nigeria and Uganda. From these examples, cyber-harassment provisions in Nigeria and Uganda are similarly worded to Section 27 of the CMCA. Crucially, they have been documented as being used by the respective governments to suppress opposition, (Adibe, 2015, p. 123; Rukundo, 2018) giving credence to the fear that such laws could stifle legitimate criticism.

This paper argues that Section 27 of the CMCA is overbroad and poses a risk to the freedom of expression. In particular, this overbreadth has the potential to endanger political speech that is often vital to democratic participation. It argues that in upholding the constitutionality of the provision, the High Court made an error of judgment. Aside from this, the paper argues that the law fails to capture different forms of harassment. It proceeds in five parts, including this introduction. In part two, the concept of cyber-harassment is defined with a view to elucidating the reasons for its inclusion as a limit to the freedom of expression. Part two also reviews Kenya's legislative process to point out the absence of a clear policy guiding the enactment of Section 27, and the resulting inconsistency with the freedom of expression. Drawing on this discussion, part three criticises the decision of the High Court upholding Section 27. By juxtaposing the High Court's decision to the same court's earlier ruling on Section 29 of KICA, this paper argues that Section 27 is overbroad, and poses a substantial risk to

the freedom of expression. Using the examples of Nigeria and Uganda, both of which have similarly worded cyber-harassment laws, constitutional provisions on the freedom of expression, and limitation clauses, this paper finds, in part four, that this risk is particularly manifest in relation to political speech. In part five, the paper concludes with some considerations Kenya ought to make when dealing with online harassment.

2. CYBER-HARASSMENT

Before delving into Kenya's cyber-harassment provision, this part discusses the concept of cyber-harassment generally. In order to understand the nature of the offence, two primary approaches to conceptualising harassment are identified. The first is a nuanced approach that recognises the different forms of harassment and their components. The second is a blanket approach that focuses on repetition as the primary component of all forms of harassment. The law's response to this offence is then discussed, identifying two primary responses: the application of general laws such as criminal law, and of cyber-specific laws. In the second part, the legislative process that led to the offence in the CMCA is highlighted. This review of the previous iterations of the offence points to an absence of clarity on what forms of harassment the CMCA aimed to deal with. In doing so, the part highlights the law's incompatibility with the stated objectives and the freedom of expression.

2.1. What is Cyber-Harassment?

According to Crootof and Ard, developments in technology sometimes upend existing frameworks and engender legal uncertainties which regulators have to contend with. Questions abound regarding the suitability of extant laws, and the extent to which one ought to direct laws or regulations at specific technologies (Crootof & Ard). How states have attempted to address online harassment is an example of this. Harassment is not a novel offence and legal remedies lay in tort, libel, and sometimes criminal law in a number of jurisdictions (Citron, 2014,

p. 120). However, the advent of the networked society has exacerbated already existing concerns of harassment (Shmyla, 2017, p. 8). For example, cyber-harrassment is gendered in nature with women often falling prey to, among other things, revenge porn and cyber bullying (Shmyla, 2017; Citron, 2014; Citron, 2010). The responses to this exacerbation have been categorised in two ways by Shmyla (2017): a trend toward legislation specifically addressing online harassment, and a belief that online harassment is simply a mirror of offline behavior resulting in the application of existing laws (Crootof & Ard). With the nature of the Internet being cited as fomenting echo chambers and emboldening already nefarious groups (Citron, 2010, p. 36-37), the desire for the former response, namely, cyber-specific legislation explicitly defining the offence, is understandable. At its most extreme, cyber-harassment may result in victims committing suicide, but more often leads to emotional distress (Laer, 2014, p. 85), which is also very problematic. Some countries lacking legislation that directly addresses cyber-harassment have modified extant statutes prohibiting harassment, adding language specifying that contact made on the Internet and other digital devices may also constitute harassment (Hazelwood & Koon-Magnin, 2013, p. 156). The definition of "harassment" in South Africa's Protection from Harassment Act, for instance, extends to harmful electronic communications (Protection from Harassment Act 2011, s. 1). Other countries have distinctly legislated for cyber harassment (Hazelwood & Koon-Magnin, 2013, p. 156). In light of the novelty of cyber-harassment legislation and the varying approaches taken to address the offence, there is no consensus on a common definition of cyber-harassment currently (Hazelwood & Koon-Magnin, 2013, p. 156). However, attempts have been made to define cyber-harassment.

In attempts to define it, there have generally been trends towards either of two approaches. In both, cyber-harassment refers to offensive communication/conduct that takes place online i.e., through emails, texts and other forms of electronic communication (European Institute for Gender Equality). Such offensive

communication includes messages/conduct that "intentionally humiliate, annoy, attack, threaten, alarm, offend and/or verbally abuse individuals" (UN Office on Drugs and Crime). However, the first approach, in dealing with harassment, goes beyond this broad conception. It adopts, a more nuanced approach of appreciating the components of the different offences. As a result, hate speech, revenge porn, online impersonation, cyberstalking, doxing (the intentionally searching for and leaking of someone's private information), and trolling are all considered types of harassment that can take place online each with different thresholds for criminality (Strickland, 2017). Crucially, these distinctions are clearly defined i.e., the law distinguishes one form of harassment from another with regard to the actus reus and mens rea. However, not all laws implement this categorisation, as will be seen in the second part, in which Kenya's law is discussed.

In the second approach, cyber-harassment is used only to refer to instances where offensive communication is repetitive or comprises a pattern and would cause a reasonable person apprehension (Smith, 2018, p. 1563; Citron, 2015, p. 2). This approach does not move past the broad understanding of cyber-harassment as offensive communication that takes place online. It does not consider that one form of offensive communication may be graver than another, and thereby call for a higher threshold of criminality. It often uses the terms 'cyber harassment', 'cyber-stalking', and 'cyber-bullying' interchangeably, using one of the terms to encompass all these forms of harassment (Jameson, 2009; Fukuchi, 2011, p. 292). This approach is exclusionary in that it fails to take into account the varied forms of harassment that may take place in a single (one-off) instance such as revenge porn or hate speech. If one were to exclude these from harassment law by providing for them in a specialised law (as is the case for hate speech, and increasingly, revenge porn) then this approach may be suitable. As opposed to appreciating the nature of each type of harassment, this approach focuses on the harm engendered by the repetitive nature of what is deemed to be offensive communication.

Generally, laws prohibiting harassment entail the classification of certain types of speech or conduct as illegal. Opponents of these laws often argue that such restrictions run counter to the freedom of expression (Citron, 2010, p. 190). The freedom of expression guarantees the right to seek, receive and impart ideas of any kind (ICCPR, a. 19; Constitution of Kenya 2010, a. 3).[2] To free speech absolutists, anything short of a blanket permissibility of speech amounts to a violation of this freedom, or would have a chilling effect on it.[3] However, the matter is much more nuanced. In discourse, some speech is considered of 'low value' i.e., not contributing to society sufficiently to warrant protection (Citron, 2010, p. 196). Appreciating that free speech has been recognised as important for purposes of safeguarding democracy, personal autonomy and the advancement of knowledge (Tsesis, n.d., p. 2), it is easy to write off instances of cyber-harassment as 'low value' contributions to this end, and thus justify their limitation (Citron, 2010, p. 200; *Watts v. US*, 1969*; Giboney v. Empire Storage*, 1949).[4] However, such limitations ought to adhere to whatever legal test is enumerated in the various jurisdictions for the curtailment of constitutional freedom. Around the world, the most common is that the limitation be prescribed by law, in pursuit of a legitimate aim that is necessary in a democratic society and must manifest itself in the least restrictive means possible (ICCPR, a. 19(3)). In Kenya, this is provided for in Article 24 of the Constitution (2010), which is discussed below.

2.2. Cyber-Harassment in Kenya

From a reading of Section 27 of the CMCA, Kenya appears not to have a consistent conceptual approach to cyber-harassment. The offence does not make any distinction between the varied forms of

[2] This freedom is subject to varied applications in different countries. In Kenya, it is protected under Article 33 of the Constitution of Kenya (2010).

[3] The concept of chilling effect refers to a deterrence of people exercising the right/freedom in question due to fear of legal liability or other consequences prescribed by the law limiting the right.

[4] In the United States (US), two types of speech can fall in this category, true threats (*see Watts v. United States* 394 US 705 (1969)) and speech integral to criminal conduct.

harassment, nor does it emphasise on repetition of a particular harmful conduct as being the main component. Through reviewing the previous drafts of Section 27 when the CMCA was undergoing Parliamentary debate, this part highlights the underwhelming attempts by legislators to address both the intended aim of the law and the potential risk to the freedom of expression.

As mentioned in the previous part, remedies for harassment often lay in tort, libel or criminal law. Kenya is no exception. Prior to the CMCA, there were not any clear-cut means to address bullying or harassment other than through a tortious action or civil claim (*e.g.* of defamation) (Laibuta, 2019 June 20). Previous attempts to address harmful communication have been unsuccessful. For example, both Section 29 of KICA and the offence of criminal defamation under the Penal Code were invalidated by the High Court (*Geoffrey Andare v. AG*, 2016).[5] The National Cohesion and Integration Act (2008), while dealing with harmful speech, focuses only on hate speech and ethnic/racial contempt (s. 13 & 62). The fact that existing laws were not fit for purpose was recognised during the National Assembly's second reading of the CMCA (then referred to as the 'Computer and Cybercrimes Bill') (National Assembly Hansard, 2018 March 21, Afternoon Sitting, p. 26). From the eventual assent of the Bill into law, it is clear that Kenya opted to remedy this by creating a law targeting online harassment specifically. However, the provision that was enacted appears to be an attempt to address a broader definition of cyber-harassment, covering all forms of 'offensive' communication, though not recognising the nuanced nature of each offence. Throughout parliamentary debate, there were instances of MPs conflating different kinds of offences, and assuming that the enactment of a provision entitled 'cyber-harassment' would be a panacea (National Assembly Hansard, 2018 March 21, Afternoon Sitting). The incoherence of this attempt at conceptualising the offence, and the absence of a clear understanding of the harms in question, are best captured by the amendments made during debate.

[5] Section 194 of the Penal Code of Kenya criminalised the intentional and unlawful publication of defamatory content concerning another person.

2.2.1. Amendments

Prior to the CMCA's assent, when it was a Bill before Parliament, the offence of cyber-harassment was referred to as 'cyber-stalking and cyber-bullying' and read as follows:

> 16. (1) Any person who, individually or with other persons, willfully and repeatedly communicates, either directly or indirectly, with another person or anyone known to that person, commits an offence, if they know or ought to know that their conduct—
> (a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that person's property; or
> (b) detrimentally affects that person. (cl. 16 (1)).[6]

The Bill proceeded to set out exceptions in Clause 16(3), namely, a public interest defence, conduct in compliance with the law, and the pursuit of a crime. From the record of parliamentary debate, it is salient that many MPs were concerned about their own experiences with a number citing instances when they were harassed through social media (National Assembly Hansard, 2018 March 21, Afternoon Sitting, p. 13, 31, & 37). Generally, the MPs were of the opinion that social media has been leveraged by people to advance attacks against others and therefore sought to enact this particular provision to provide a specific remedy for the victims. However, there was no discussion on the nature of the different forms of harassment that existed or that the legislators sought to address in particular.[7]

The provision's incongruence with the freedom of expression was noted by one MP who went on to suggest that the clause was unclear and could risk stifling legitimate criticism (National Assembly Hansard, 2018 March 21, Afternoon Sitting, p. 23). An

[6] There are two earlier version of this Bill, the first drafted in 2014 and found here: https://www.article19.org/wp-content/uploads/2018/02/Kenya-Cybercrime-Bill-129072014-BB.pdf and the in 2016: https://www.article19.org/data/files/medialibrary/38561/Analysis-Kenya-Computer-and-Cybercrimes-Bill-2016.pdf however they are not discussed in this commentary as they were not tabled before Parliament.

[7] The types of harassment complained of by the legislators varied widely. Some were repetitive in nature, such as bloggers publishing falsehoods about them on social media platforms on a regular basis, and some were one-off, such as nude images being sent to them via WhatsApp. Despite recognising this, there was a failure to taxonomise these forms of harassment by the MPs.

international free speech advocacy group took issue with the wording of the clause, suggesting that metrics such as "apprehension or fear of violence" set a low bar for criminality and opened up opportunities for political suppression (Article 19, 2018, p. 16). Further, the vague expression "detrimentally affects that person" was described as broad (Article 19, 2018, p. 16). The free speech advocacy group was also of the opinion that cyber-stalking and harassment ought to be dealt with using general criminal law as opposed to cyber-legislation (Article 19, 2018, p. 16).

During the third reading in Parliament, key amendments were made including, a change in the marginal note, and the deletion of the words 'and repeatedly" (National Assembly Hansard, 2018 April 26, Morning Sitting, p. 17). The outcome of this was Section 27 of the CMCA (now entitled 'cyber harassment'), which reads:

> 27(1) A person who, individually or with other persons, willfully communicates, either directly or indirectly, with another person or anyone known to that person, commits an offence, if they know or ought to know that their conduct—
>
> (a) is likely to cause those persons apprehension or fear of violence to them or damage or loss on that person's property; or
>
> (b) detrimentally affects that person; or
>
> (c) is in whole or part, of an indecent or grossly offensive nature and affects the person.

Despite criticism that the thresholds put in place for commission of the offence were too low, and that the wording was too broad, Parliament largely maintained it. In fact, the final wording expanded the scope of the offence by removing the requirement that the communication be repetitive in nature and including vague terms such as "…and affects the person" in sub clause (1)(c). In addition to this, all the exceptions previously listed in Clause 16(3) were removed. The scope of the offence, coupled with the weight of the penalty—a KES 20 million fine, or a 10-year term of imprisonment, or both, which is among the most severe of penalties in Kenyan law—raise the concern that this provision

could have a chilling effect on the freedom of expression (Laibuta, 2019).

Under Section 27, it appears as though anyone who simply sends out a message that affects the recipient subjectively commits an offence. Would this encompass legitimate criticism? Would it apply to satire or parody that touches one's nerve but is legitimate speech? The line is not clear. Even if one were to take the intent of the law into account—mitigation of online harassment—the use of this provision is imprecise and overbroad. Not only does it overshoot its objective of limiting harmful speech, it also fails to appreciate the gravity of varied forms of harassment clearly. For example, cyber-stalking, which requires repetition of harmful and offensive communication, would be punishable under Section 27 (at the first instance of transmission, even before subsequent instances) and attract the same penalty as a singular message, despite the latter being typically less harmful. Such overbroad laws always run the risk of being abused, and in other jurisdictions such as Pakistan, have been used to further political ends (Shmyla, 2017). These were some of the arguments raised by BAKE in its Petition to the High Court.

2.2.2. Cyber-Harassment and the Freedom of Expression in Kenya

BAKE challenged most of the provisions at the High Court on the basis that they limited the freedom of expression under Article 33 unconstitutionally (*BAKE v. AG*, 2020). The freedom of expression in Kenya does not extend to propaganda for war, incitement to violence, hate speech, or advocacy of hatred (Constitution of Kenya 2010, a. 33 (2)). Perhaps with the exception of hate speech, cyber-harassment, as described in the CMCA, does not fall within the exceptions listed in Article 33, and such speech is arguably protected. However, as stated in the previous part, where certain speech is of "low value", limitation is justifiable.

The constitutionality of limits such as Section 27 of the CMCA ought to be determined on the basis of the test in Article 24 of the

Constitution. The Constitution of Kenya (2010) requires that a constitutionally protected right

> "…shall not be limited except by law, and then only to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors…" (a. 24).

The Article provides examples of relevant factors: the nature of the right, the importance of the aim, the nature and extent of the limitation, the risk posed to the enjoyment of rights, and the proportionality of the limitation (Constitution of Kenya 2010, a. 24). Therefore, limitations may be unconstitutional either due to their purpose, or their effect on a constitutionally protected right (*Olum and another v. Attorney General*, 2002). It is not in dispute that curbing harassment is a valid purpose. However, the effect of this law is what the High Court ought to have considered in the BAKE Petition, which is discussed in the next part of this paper.

3. The High Court on Section 27 of the CMCA

This part argues that Justice Makau, in his ruling on the BAKE Petition, erred in his finding on the constitutionality of the limits imposed by Section 27 of the CMCA. Three main issues arose in relation to the offence of cyber-harassment: (a) its absence on the list of exceptions to the freedom of expression in Article 33; (b) its similarity to Section 29 of KICA previously declared unconstitutional; and (c) the burden to prove the existence of less restrictive means. These three issues are discussed in this part. It concludes that Justice Makau's analysis failed to appreciate the limitations test as enumerated in Article 24 and developed by Justice Ngugi in *Geoffrey Andare v Attorney General,* where Section 29 of KICA was invalidated.

3.1. Section 27 as an Exception to the Freedom of Expression

In the petition, BAKE argued that Article 33 contains an enumerated list of exceptions to the freedom of expression. In light

of the absence of cyber-harassment from that list, they contended that the limitation imposed by the CMCA was unconstitutional, tying this in with the argument that cyber-harassment was similar to Section 29 of KICA (*BAKE v. AG*, 2020).

In response, the court noted that aside from the exceptions in Article 33, the Constitution permits the limitation of the freedom of expression under Article 24 provided that the aim sought is a legitimate one, and the process adhered to, a legal one. It went ahead to suggest that the objective of Section 27 was a sound one in the context of the "socially harmful conduct" that is harassment (*BAKE v. AG*, 2020). This finding is unproblematic as criminalising cyber-harassment does entail pursuing a legitimate social aim.

3.2. Cyber-Harassment, KICA and the Overbreadth Doctrine

In 2016, Justice Ngugi, in *Geoffrey Andare v. the Attorney General*, declared Section 29 of the KICA—on the improper use of a licenced communications system—unconstitutional. According to BAKE, Section 27 of the CMCA criminalised speech in a similar manner to Section 29 of KICA and as a result, ought to have been declared unconstitutional.

There are two main similarities between the wording of Section 27 of the CMCA and Section 29 of the KICA: both offences deal with online communication, and both include the use of undefined terms such as 'indecent', 'offensive' and 'obscene'. In *Geoffrey Andare*, Justice Ngugi declared Section 29 unconstitutional due to its broad nature, arguing that the difficulty in foreseeing liability, and the reliance on subjective interpretation would have created a chilling effect on the freedom of expression. Justice Makau, in the BAKE Petition, held that the offences—of cyber-harassment and improper use of a licenced communications system—differed on the basis of the target of the law. The CMCA applies to individuals using any computer system, while the KICA only applied to licensees under its framework (*BAKE v. AG*, 2020, para. 71). While this finding is factually true, it should not have precluded further analysis on whether the wording of the law

conformed to the level of certainty required of limitations (*Geoffrey Andare v. AG*, 2016). Such analysis would have revealed the overbroad nature of the provision. Limitations on constitutionally guaranteed freedoms must be clearly prescribed by law (Constitution of Kenya 2010, a. 24 (1)). Such prescription ought to engender certainty; the subjects of the law ought to be able to foresee liability for their actions. Where the limitation is broad and worded vaguely, it runs the risk of having a chilling effect on the freedom in question (*Geoffrey Andare v. AG*, 2016). The use of similarly vague phrases in Section 27 of the CMCA raises the valid concern that the law is overbroad.

3.3. Proportionality of Section 27 of the CMCA

BAKE did not raise the issue of whether there were less restrictive means to achieving the objectives of Section 27 directly. However, the High Court bundled the issue with its findings on the validity of the aim sought by the offence. Justice Makau held that not only was Section 27 valid in light of the socially harmful nature of cyber-harassment, but also that the Petitioner failed to show that it was an unnecessary provision in light of the existence of less restrictive means of achieving the aim (*BAKE v. AG*, 2020, para. 74). These findings fall short on two fronts. On the first, the discussion should have surpassed the necessity of Section 27 and delved into its proportionality - the very essence of searching for a less restrictive means. On the second, the burden to prove the existence of a less restrictive means should not have fallen on the Petitioner but the State.

While the High Court was right in finding that there was no law catering for cyber-harassment directly (barring the fact that harassment in and of itself has existing legal remedies), the question at hand goes beyond mere necessity and delves into the precision and proportionality of the approach taken. Taking Section 27 of the CMCA as necessary and lawful simply due to the inexistence of less stringent alternatives appears as though the High Court implied that it is impossible for Parliament to amend

the provision in favour of a narrower and more lenient one; that as long as there are no alternatives, Parliament would be free to enact overbroad and harsh offences that would then be found to withstand constitutional scrutiny. The Act, as worded, permits the enforcement of a vague and overbroad provision with the threat of a hefty penalty. The potential chilling effect on the freedom of expression is clear. It is further compounded in politically charged contexts. In a recent conference, in response to the Chief Justice of Kenya's complaints of harassment by bloggers, the President of Kenya responded that courts have always nullified the Government's attempts to rein in bloggers by declaring laws unconstitutional (Agutu, 2019) - potentially rousing suspicion regarding the veracity of the often-stated noble objectives of these laws.

As for the burden of establishing the existence of less restrictive means, Justice Makau argued that the Petitioner had failed to do so (*BAKE v. AG*, 2020, para. 73). However, this was an error on the court's part. According to Article 24 of the Constitution, the responsibility to ensure that fundamental rights are limited using the least restrictive means falls on the State squarely. Further, when such restrictions are challenged subsequently, the mere claim that the law in question is invalid places a burden on the State to prove that, in advancing its legitimate aim, it chose the least restrictive means (*Geoffrey Andare v. AG*, 2016, para. 96). Even where the State fails to do this, the High Court, itself, undertakes this analysis in rendering its decision (*Okiya Omtatah Okoiti v. CAK*, 2018) - the burden should not be placed on petitioners (*Geoffrey Andare v. AG*, 2016, para. 98). In this case, the State did not prove that existing civil and criminal laws are unfit for purpose despite what was stated during parliamentary debate, and neither did the court conduct an investigation into the existing legal framework to assess the State's adherence to the test in Article 24.

While it is well within the rights of governments to secure the wellbeing of their citizens by limiting 'low-value' speech, the dangers of overbroad limitations are clear where the government

enforces these laws with a heavy hand. Kenya's cyber-harassment provision is yet to be tested as the law only recently became operational. However, Nigeria and Uganda have similar laws, and from their experiences one can discern the potential harm of applying such laws *viz,* suppression of political speech. The following part highlights how Nigeria and Uganda have grappled with overbroad laws.

4. Nigeria and Uganda: Political Speech Under Cyber-Harassment Laws

4.1. Nigeria

In Nigeria, cyber-harassment is a generic term and the Cybercrimes (Prohibition, Prevention, etc.) Act (2015) details the various categories that fall under it such as hate speech, revenge porn and cyber-stalking. In Section 24, the Act describes cyber-stalking as knowingly or intentionally sending or causing the transmission of the following over a computer system or network:[8] grossly offensive messages, false messages, messages intended to bully or harass or threaten, kidnapping threats, and threats to property or reputation. Despite cyber-stalking being defined in Section 58 as an offence requiring a pattern of conduct, Section 24 is worded to allow for prosecution of one-off incidents as stalking.

The freedom of expression, including press freedom, is protected in Nigeria's Constitution (1999) and may only be limited by a law that is reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality and health, or for the protection of the rights and freedoms of other persons (s. 39). In spite of the constitutional guarantee of the freedom of expression, tolerance of contrary political views by those in Government remains low often leading to the subjection of citizens and the press to all manner of intimidation tactics including death threats, arbitrary detentions and frivolous lawsuits (Amnesty International, 2019 October 14; Adibe et al.,

[8] Paraphrased for purposes of brevity.

2017, p. 121; *Ogwuche v. Federal Republic of Nigeria*, 2018). There have been many cases of journalists and bloggers in Nigeria being charged with cyber-stalking for publishing stories deemed to be "offensive", "obstructive" "insulting" or "annoying"—often in spite of the accuracy of published stories (Adibe et al., 2017, p. 123).

Much like in Kenya, the Nigerian Cybercrimes Act uses subjective terms (Mofesomso, 2019, p. 23) such as "offensive", "obstructive", "annoying" and "insulting" to describe elements of the offence and makes no attempt to define them anywhere in the Act. Though there is yet to be a conviction under the law, it would be unconstitutional for a person to be convicted of an offence that is not defined (Constitution of Nigeria 1999, s. 36 (12) Attempts to challenge the law have been unsuccessful (*Okedara v. AG of Nigeria*, 2017).

4.2. Uganda

Uganda's Computer Misuse Act (2011) creates the offence of cyber-harassment, which it defines as: "making requests, suggestions or proposals that are obscene, lewd, lascivious or indecent; threatening to inflict injury or physical harm to the person or property of any person; or knowingly permitting any such electronic communication" (s. 24 (2)). The Computer Misuse Act also differentiates the types of cyber-harassment *e.g.* cyber-stalking and offensive communication are different offences. The Computer Misuse Act (2011) prohibits offensive communication that it describes as the willful and repeated use of electronic communication to disturb the peace and quiet or privacy of someone without any legitimate reason to communicate (s. 25). Similar to Kenya and Nigeria, terms used to describe cyber-harassment like "obscene", "lewd", "lascivious" or "indecent" have not been defined in the Computer Misuse Act, leaving their meaning open to subjective interpretation contrary to Article 28(12) of Uganda's Constitution (1995, a. 28 (12)). Similarly, the description of offensive communication is that which 'disturbs the peace of another' - also subjective. Neither the Act nor the courts have interpreted these terms. A similar provision in Uganda's

Referendum Act of 2002 that limited speech using vague terms such as "malicious", "sectarian", "abusive", "derogatory" or "insulting" was found to be vague and unconstitutional in *Rwanyarare v. Attorney General*.

The overbroad nature of these offences has been documented as resulting in their use as a tool for political suppression through the curtailment of the freedom of expression. This arguably fails to meet the standard under Uganda's Constitution (1995) that limitations of rights be acceptable and justifiable in a democratic society (a. 43). Stella Nyanzi, a Ugandan academic, human rights defender and activist, has twice been charged after making bold remarks about President Museveni and his family members on social media. In 2017, she was charged with cyber-harassment and offensive communication for referring to the President as a "pair of buttocks" (Nyanzi v Uganda, 2017). In 2018, she posted a poem on Facebook, condemning President Museveni's rule, which was deemed offensive to him and his late mother, leading to her conviction for cyber-harassment in 2019 (Aljazeera, 2019 August 3). Though she was later acquitted due to procedural technicalities, her earlier conviction demonstrates the restrictive nature of Section 24(2) of the Computer Misuse Act as it may limit certain modes of expression merely because they are considered impolite (Rukundo, 2018, p. 265; *Stella Nyanzi v. Uganda*, 2020). This is notwithstanding the fact that controversial or unpleasant expressions are not automatically exempt from constitutional protection (*Obbo v. AG of Uganda*, 2004). In fact, public officials are expected to be open to harsher criticism (*Andrew Mujuni Mwenda v. Attorney General*, 2005). The use of language that expresses disappointment in leadership should be allowable and expected as part of freedom of expression (Rukundo, 2018, p. 269).

With the examples of Nigeria and Uganda, a strong case may be made for the existing risk that Kenya's cyber-harassment law may either be used for suppression of legitimate criticism by the Government or may have a chilling effect on expression.

5. CONCLUSION

Peer to peer communications that take place electronically have exacerbated already existing ills such as hate speech, defamation and bullying markedly. It is therefore understandable that, increasingly, cyber-harassment is featuring on the legislative agenda. However, Kenya's attempt at mitigating online harassment through Section 27 of the CMCA has proven problematic on multiple fronts. On the first front, the law fails to recognise the nuance in cyber-harassment and in an attempt to create a blanket offence, excludes socially harmful conduct such as identity theft, cyber-stalking, and doxing, to name a few. On the second, the law's wording is so broad as to engender uncertainty in its applicability. As a result of this uncertainty there is the risk that the law, as worded, may be used to stifle legitimate political opposition or criticism by journalists, citizens and anyone who would seek to hold the Government accountable as has been done in countries with similarly worded laws.

In *Geoffrey Andare v Attorney General*, Justice Ngugi, citing *Arthur Papa Odera v. Peter Ekisa*, suggested that libel laws would be sufficient in protecting one's reputation when disparaged via social media (*Geoffrey Andare v. AG*, 2016, para. 98). This was in light of Section 29 of KICA's stated objective - protection of reputation. This led to the conclusion that there were less excessive means. While, the referenced libel law was declared unconstitutional in *Jacqueline Okuta v Attorney General* (2017), there are other means through which one can address harassment. Even though in the case of cyber-harassment there is a wider scope of aims (other than protecting one's reputation), there is also a wider range of recourse for victims in law. For example, general tortious claims, and for revenge porn, Section 37 of the CMCA (2018), which provides for unlawful disclosures of intimate images. It is for this reason that the civil society organisation, Article19, recommended the application of general criminal and civil law to instances of cyber-harassment (Article 19, 2018, p. 16). This would not be the most ideal scenario bearing in mind the idiosyncrasies

of networked technologies, but in lieu of a narrower cyber-crimes law that is clear in scope, it is a better alternative to risking the freedom of expression.

REFERENCES

Adibe, R., Ike, C., Udeogu, C. (2017). Press Freedom and Nigeria's Cybercrime Act of 2015: An assessment. *Africa Spectrum, 52(2).*

African Union Commission. (2016). Cybercrime and Cybersecurity: Trends in Africa.

African Union Convention on Cyber Security and Personal Data Protection. (2014).

Agutu, N. (2019 January 25). Get used to bloggers and move on, Uhuru tells Maraga. The Star.

Aljazeera. (2019, August 3). Ugandan academic Stella Nyanzi jailed for 'harassing' Museveni.

Amnesty International. (2019, October 14). Nigeria: Endangered Voices: Attack on the freedom of expression on Nigeria.

Andrew Mujuni Mwenda & Anor v Attorney General (2005), Constitutional Court of Uganda.

Article19. (2018). Kenya: Cybercrime and Computer Related Crimes Bill. *Legal Analysis*.

Bloggers Association of Kenya (BAKE) v Attorney General & 5 others (2018) eKLR.

Citron, D. (2010). Civil rights in our information age. In Levmore S. & Nussbaum M. (Ed.)., *The Offensive internet*. Harvard University Press.

Citron, D. (2014). *Hate Crimes in Cyberspace*. Harvard University Press.

Citron, D. (2015). Addressing cyber harassment: An overview of hate crimes in cyberspace. *Journal of Law, Technology & the Internet,* 6.

Computer Misuse Act (2011, Uganda).

Computer Misuse and Cybercrimes Act, n.5. (2018.).

Constitution of the Federal Republic of Nigeria (1999).

Constitution of the Republic of Uganda (1995).

Crootof, R. & Ard, B.J. (Forthcoming 2021). Structuring techlaw. *Harvard Journal of Law & Tech*, 34.

Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015 (Nigeria).

European Institute for Gender Equality. (n.d.).

Geoffrey Andare v AG & 2 others (2016) eKLR.

Giboney v. Empire Storage & Ice Co. 336 US 490 (1949).

Grayned v City of Rockford, 408 US 104 (1972).

Hazelwood, S. & Koon-Magnin, S. (2013). Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative analysis. *International Journal of Cyber Criminology*, *7(2).*

International Covenant on Civil and Political Rights (ICCPR), 19 December 1966, 999 U.N.T.S. 171, (entered into force 23 March 1976).

Jacqueline Okuta & another v AG & 2 others (2017) eKLR.

Jameson, S. (2009 May). Cyberharassment: Striking A Balance Between Free Speech and Privacy.

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, *22(2).*

Laer, T. (2014). The means to justify the end: Combating cyber harassment in social media. *Journal of Business Ethics*, *123(1).*

Laibuta, M. (2019 June 20). Cyber-bullying under Kenyan law. Mugambi Laibuta Blog.

National Assembly Hansard. (1 March 2018, Afternoon Sitting).

National Cohesion and Integration Act, n.17 (2008).

Nyanzi v. Uganda (2017), Uganda Human Rights Commission.

Obbo and another v. Attorney General (2004)1 EA 265.

Ogwuche v. Federal Republic of Nigeria (2018), Sub-regional African Courts.

Okedara v. Attorney General of the Federation (2017), Federal High Court of Nigeria.

Okiya Omtatah Okoiti v. CAK & 8 others (2018) eKLR.

Olum and another v. Attorney General (2002) 2 EA.

Protection from Harassment Act, n.17. (2011).

Rukundo, S. (2018). My President is a Pair of Buttocks': the limits of online freedom of expression in Uganda. *International Journal of Law and Information Technology,* 26.

Shmyla, K. (2017). Using criminal law to tackle cyber harassment: Conceptual and procedural pitfalls from a feminist perspective. *Pakistan Law Review*, 8(1).

Smith, S. (2018). Threading the First Amendment needle: Anonymous speech, online harassment, and Washington's cyberstalking statute. *Washington Law Review*, 93(3).

Stella Nyanzi v. Uganda (2020), The High Court of Uganda.

Strickland, P. & Dent, J. (2017 September 13). Online harassment and cyber bullying. *House of Commons Library*, No. 07967.

The Computer and Cybercrimes Bill (2017).

The Constitution of Kenya (2010).

Tsesis, A. (n.d.). Free speech constitutionalism. *Yale Information and Society Project*.

UN Office on Drugs and Crime. (n.d.). Interpersonal Cybercrime Module.

Watts v. United States (1969) 394 US 705.