ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

The Commonwealth

A Comparative Review of Cybercrime Law in Kenya: Juxtaposing National Legislation with International Treaty Standards

Brian Sang YK[1] and Ivan Sang[2]

Abstract

The enactment of Kenya's first comprehensive cybercrime legislation, the Computer Misuse and Cybercrimes Act 2018 ('Cybercrimes Act'), was a significant milestone in laying down legal regulations for cyber-activities. Two international treaty instruments – namely, the Budapest Convention on Cybercrime and the African Union Convention on Cyber Security and Personal Data Protection – were influential in drafting the Cybercrimes Act. Yet some of the provisions of the Cybercrimes Act that establish key definitions and criminal offences are inconsistent with these international treaty standards and in breach of Kenya's Constitution. This article argues that, if not reformed, these defective provisions run the risk of (i) interfering with digital rights and (ii) undermining the efficacy of Kenya's cybercrime law. To systematically make the case for reform, this article comparatively reviews sections of the Cybercrimes Act by juxtaposing them with their equivalents in international treaties and selected national laws. The article proposes amendments to the Cybercrimes Act so as to result in a much more effective regime of cybercrime law in Kenya.

1 Advocate of the High Court of Kenya; Deputy Director, Administrative Services, County Government of Narok, Kenya. Email: briansang.yk@gmail.com
2 Senior Researcher, Office of the Deputy Vice-Chancellor Research & Innovation, Strathmore University (Nairobi, Kenya). Email: isang@strathmore.edu

1. Introduction

Like many comparable Commonwealth member countries, Kenya is significantly affected by cybercrime, owing to the increasing reliance on internet-driven services without a corresponding improvement in legal regulations.[3] As a result of the rapid digitisation in Kenya from the late 2000s,[4] the incidence of cybercrime has grown exponentially and it is now estimated to cost the Kenyan economy more than US$210 million annually.[5] Computer systems, devices and tools have been used to fraudulently obtain and launder both public and private funds.[6] Social media networks have also been used to spread hate speech and disinformation, to incite violence and to launch malicious personal or political attacks.[7] Hackers have even leaked classified government records, including a terabyte of private personnel biodata from Kenya's Ministry of Foreign Affairs.[8] Another variant of cybercrime is the insidious use of online platforms to indoctrinate vulnerable Kenyans into violent extremist belief systems, which often results in deadly terrorist activity.[9]

This context underscores Kenya's technological exposure and the extensive impact that cybercrime has on its socio-economic stability and national security.[10] It also underlines the need for a robust cybercrime law in Kenya. As such, the enactment of Kenya's comprehensive cybercrime law, the Computer Misuse and Cybercrimes Act 2018 ('Cybercrimes Act'),[11] was a creditable legislative step in setting out the legal framework for tackling criminal activities online. International treaties – namely the Council of Europe Convention on Cybercrime ('Budapest Convention on Cybercrime')[12] and the African Union Convention on Cyber Security and Personal Data Protection ('Malabo Convention on Cyber Security')[13] – were influential in drafting the Kenyan Cybercrimes Act. Yet, for all the progressive normative contributions of these two international treaties, several provisions of the Kenyan Cybercrimes Act are problematic. This article critiques these defective provisions, which it shows to be inconsistent with both the international treaty standards and Kenya's constitutional rights guarantees.

3 Kshetri, N. (2019) 'Cybercrime and Cybersecurity in Africa'. *Journal of Global Information Technology Management* 22(2): 77–81.
4 Rutenberg, I. (2018) *Cyber Law in Kenya*. Philadelphia, PA: Wolters Kluwer.
5 Serianu (2017), *Kenya Cyber Security Report 2017*. Nairobi: Serianu.
6 Leftie, P. (2016) 'How Officials Manipulate IFMIS to Steal Public Funds' *Daily Nation,* 27 November. www.nation.co.ke/news/1056-3466304-5fes0sz/index.html
7 BAKE (2018) *State of the Internet in Kenya 2017*. Nairobi: BAKE.
8 TESPOK (2017) *Cyber Threats Report 2016*. Nairobi: TESPOK.
9 Government of Kenya (2016) *National Strategy to Counter Violent Extremism*. Nairobi: Government of Kenya.
10 UNECA (2014) 'Tackling the Challenges of Cybersecurity in Africa'. Policy Brief. Addis Ababa; UNECA.
11 Act No. 5 of 2018. This Act is referred to as a comprehensive cybercrime law because it has consolidated and updated the earlier disparate laws that governed improper use of communication devices and computer-related offences. In addition, the Act sets out for the first time an institutional framework for holistic co-ordination at the national level of the detection, prohibition, prevention, response, investigation and prosecution of cybercrimes, as well as for the facilitation of international co-operation in tackling cybercrimes.
12 ETS No. 185 (entered into force 1 June 2004).
13 EX.CL/846(XXV) (adopted 27 June 2014).

This article argues that, if not reformed, these defective provisions run the risk of interfering with digital rights and undermining the efficacy of Kenya's cybercrime law. In doing so, it critically assesses the content of Kenya's Cybercrimes Act relating to the criminalisation of cyber-conduct and draws attention to the ways in which the Act can be reformed. This analysis is made in light of a recent judgement in *Bloggers Association of Kenya (BAKE) v Attorney General and 3 Others* in which the High Court of Kenya considered a constitutionality challenge against more than one-third of the sections in the Cybercrimes Act.[14] Although the Court in the *BAKE* judgement held that the challenged sections were constitutionally valid,[15] thereby overturning an earlier court decision to suspend the implicated sections,[16] this article argues that there are cogent reasons to warrant the reform of Kenya's Cybercrimes Act. The article systematically advances the case for the reform of particular provisions of the Act by means of a constructive and comparative critique.

In order to systematically demonstrate the need for amendments to problematic definitions, criminal offences and penalties in Kenya's Cybercrimes Act, this article comparatively reviews the defective sections of the Act by juxtaposing them with their equivalents in the Budapest Convention on Cybercrime and the Malabo Convention on Cyber Security. Besides international treaties, the Kenyan Cybercrimes Act is compared with national cybercrime legislation from selected Commonwealth member countries. The national jurisdictions included in this comparative legal analysis are Nigeria, South Africa, New Zealand and the United Kingdom. These jurisdictions were selected on the basis of the high degree of comparability of their respective national cybercrime laws with the Kenyan Cybercrimes Act in terms of the domestic reception of the provisions of the Budapest Convention and, where applicable, the Malabo Convention.

The main aim of this comparative review of Kenya's cybercrime law is twofold: (i) to objectively compare the provisions of the Cybercrimes Act with the legal standards reflecting international best practice; and (ii) to propose concrete amendments to the defective sections of the Act. Structured in three parts, the analysis in this article proceeds as follows.

First, it provides a brief overview of the Kenyan Cybercrimes Act so as to put the subsequent discussion of the current cybercrime law into perspective. Secondly, it evaluates the operative terms and key definitions of Kenya's Cybercrimes Act in light of the international treaty standards in the Budapest Convention and the Malabo Convention. Thirdly, it juxtaposes the substantive offences and sanctions in the Cybercrimes Act vis-a-vis comparable treaty standards in the Budapest Convention and the Malabo Convention. The comparative analysis in the third part also draws on

14 [2020] eKLR.
15 Ibid., para. 150.
16 *Bloggers Association of Kenya (BAKE) v Attorney General and 5 Others* [2018] eKLR, para. 31.

comparable legislation and case law from Nigeria, South Africa, New Zealand and the United Kingdom. The final part synthesises the article's key findings and offers some proposals on the way forward.

2. Overview of the Kenyan Cybercrimes Act

The Kenyan Cybercrimes Act clarifies in its explanatory memorandum the intention of its drafters to 'provide for offences related to computer systems; to enable timely and effective detection, investigation and prosecution of computer and cybercrimes; to facilitate international cooperation in dealing with computer and cybercrime matters; and for connected purposes'. Read as a whole, the Kenyan Cybercrimes Act has two closely related aims: (i) to protect the confidentiality, integrity and availability of computer systems, programs and data; and (ii) to facilitate the detection, investigation, prosecution and punishment of cybercrimes. The Act is divided into seven distinct parts and their content is briefly summarised below.

Part I (sections 1–3) sets out the preliminary provisions, including the definition of terms and objects of the Act. Part II (sections 4–13) provides for the establishment and modalities of the National Computer and Cybercrimes Co-ordination Committee. Part III (sections 14–46) stipulates the substantive criminal offences, detailing specific cybercrimes as well as the matching penalties. Part IV (sections 47–56) establishes the relevant investigatory and procedural powers applicable to computer-related offences and cybercrimes, including specific provisions relating to search and seizure of computer data, interception and retention of data, and evidential aspects of such data. Part V (sections 57–65) outlines the framework for international co-operation in relation to the investigation and prosecution of cybercrimes, which often have transnational elements. Part VI (sections 66–69) deals with general provisions, including the priority clause and consequential amendments. Part VII (section 70) specifies how statutory powers conferred by this Act may be delegated.

The provisions of Part III and Part IV are the focus of the present analysis as they jointly stipulate the criminal offences and their penalties, as well as the related investigatory and procedural powers. Before the Act became operational, the Bloggers Association of Kenya (BAKE) filed a petition challenging its constitutionality on the basis that it violated and threatened fundamental rights guaranteed by the Constitution.[17] The petitioners

17 *BAKE v Attorney General and 5 Others* [2018] eKLR.

specified 26 sections[18] of the Act that cumulatively infringed on the right to privacy, freedom of expression, freedom of media and access to information, the right to a fair trial and equality protections. As regards relief, the petitioners sought conservatory orders to suspend the entry into force of the specified sections of the Act until the merits of the petition were determined.

In May 2018, the High Court per Mwita J granted interim conservatory orders and suspended the operation of the 26 contested sections pending hearing and determination of the petition.[19] That suspension was lifted in February 2020, when the High Court, per Makau J, dismissed the petition.[20] The effect of that judgement was to render the Cybercrimes Act fully effective in its entirety. This article disagrees with that finding but a detailed review of the *BAKE* decision far exceeds the scope of its analysis. Instead, the aim here is to offer a comparative analysis of key definitions and offences in the Cybercrimes Act. Even so, necessary reference will be made to the *BAKE* decision when discussing elements of particular offences in the Cybercrimes Act.

To ensure an objective assessment of the merits and defects of the Kenyan Cybercrimes Act, it is necessary to juxtapose the relevant sections of the Act with selected international treaties and national laws.[21] The discussion in Sections 3 and 4 of this article critiques the selected provisions of the Cybercrimes Act that have the most comparative relevance beyond Kenya. Besides the Budapest Convention on Cybercrime and the Malabo Convention on Cyber Security, the Act is juxtaposed with Nigeria's Cybercrimes (Prohibition, Prevention, Etc) Act 2015[22] and South Africa's Cybercrimes Act 2020.[23] Sections 3 and 4 of the article also refer to the case law of the United Kingdom and New Zealand as an aid to the comparative analysis of the Cybercrimes Act.

18 The challenged sections of the Kenyan Cybercrimes Act are as follows: 5 (composition of the Committee); 16 (unauthorised interference); 17 (unauthorised interception); 22 (false publication); 23 (publication of false information); 24 (child pornography); 27 (cyber-harassment); 28 (cyber-squatting); 29 (identity theft and impersonation); 31 (interception of electronic messages or money transfers); 32 (wilful misdirection of electronic messages); 33 (cyber-terrorism); 34 (inducement to deliver electronic message); 35 (intentionally withholding message delivered erroneously); 36 (unlawful destruction of electronic messages); 37 (wrongful distribution of obscene or intimate images); 38 (fraudulent use of electronic data); 39 (issuance of false e-instructions); 40 (reporting of cyber-threat); 41 (employee responsibility to relinquish access codes); 48 (search and seizure of stored computer data); 49 (record of and access to seized data); 50 (production order); 52 (real-time collection of traffic data); and 53 (interception of content data).

19 *BAKE v Attorney General and 5 Others* [2018] eKLR, para. 33.

20 *BAKE v Attorney General and 3 Others* [2020] eKLR, para. 150 (a): 'The Computer Misuse and Cybercrimes Act 2018 is valid and does not violate, infringe or threaten fundamental rights and freedoms.'

21 Mwiburi, A.J. (2018) *Preventing and Combating Cybercrimes in East Africa: Lessons from Europe's Cybercrime Frameworks*. Berlin: Dunker & Humboldt.

22 Hereafter 'Nigerian Cybercrimes Act 2015'.

23 Hereafter 'South African Cybercrimes Act 2020'.

3. Operative terms and key definitions in the Cybercrimes Act

The interpretation of terms is a crucial determinant of the effect of words in the broader scheme of the application of law.[24] An examination of how section 2 of the Kenyan Cybercrimes Act defines certain operative terms yields a mixed report. Some terms are defined in line with international best practice; others are less well defined and may result in problematic outcomes; still others are not defined at all. A few of the definitions that reflect this assessment are discussed below.

One of the key terms used repeatedly in the Kenyan Cybercrimes Act is 'computer system'. section 2 of the Act defines this as consisting in a:

> *physical or virtual device, or a set of associated physical or virtual devices, which use electronic, magnetic, optical or other technology, to perform logical, arithmetic storage and communication functions on data or which perform control functions on physical or virtual devices including mobile devices and reference to a computer includes reference to part of a computer system.*

This definition aligns with the equivalent definition in the Budapest Convention on Cybercrime. Article 1 of the Budapest Convention defines a computer system as 'any device or a group of interconnected or interrelated devices, one or more of which, pursuant to a program, performs the automatic processing of data'. Despite the similarity, though, the definition in section 2 of Kenya's Cybercrimes Act neglects to refer to automatic processing of data as one of the key functions of a computer system. This omission is a significant shortcoming as the Act then fails to take account of developments in artificial intelligence, to indicate that automatic processing of data will be the predominant element of computer systems as automated capabilities continue to advance.[25] Current trends in social media technology that make it possible to leverage automatic data processing and the rapid evolution of big data analyses illustrate these developments.[26]

The definition of 'computer system' in the Malabo Convention on Cyber Security (in article 1) is overly technical and may not provide meaningful guidance for amending the Kenyan Cybercrimes Act.[27] In contrast, the equivalent definition in the Budapest Convention on Cybercrime presents a more pliable model that can be adopted with advantage in Kenya. It is also relevant that the Nigerian Cybercrimes Act 2015 (section 42) and South Africa's Cybercrimes Act 2020 (section 1(1)) both implicitly refer to the capability of automatic

24 Hutton, C. (2009) *Language, Meaning and the Law*. Edinburgh: Edinburgh University Press.

25 Zou, W., Xu, D. and Yu, J. (2012) 'Embedded Vision Positioning System Based on ARM Processor' in Xu, D. (ed.) *Embedded Visual System and Its Application on Robots*. Bentham Books.

26 Roosendaal, A., Kert, M., Lyle, A. and Gasper, U. (2016) 'Data Protection Law Compliance for Cybercrime and Cyberterrorism Research', in B. Akhgar and B. Brewster (eds) *Combating Cybercrimes and Cyberterrorism: Challenges, Trends and Priorities*. Springer; Council of Europe (2010) 'The Protection of Individuals with Regard to Automatic Processing of Data in the Context of Profiling'. Recommendation CM/Rec(2010)13, adopted 23 November.

27 Jamil, Z. (2016) 'Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime'. Technical Report for GLACY+.

processing of data in their respective definitions of a computer system. This reflects a modicum of consensus on the need to include the automatic data processing function in the definition of computer systems.

The Kenyan Cybercrimes Act also refers repeatedly to 'authorised person' in reference to individuals variously empowered to exercise powers or undertake such procedures as may be necessary for effective detection, investigation and prosecution of cybercrimes.[28] Yet this term is defined as 'a person designated by the Cabinet Secretary responsible for matters relating to national security by notice in the Gazette' to give effect to the investigative procedures outlined in Part IV of the Act (Section 2). By failing to specify clearly the individuals who may be regarded as authorised persons, the Cybercrimes Act gives too much discretion to the cabinet secretary.

This is problematic in light of the coercive and intrusive powers that part iv of the act gives the cabinet Secretary. Previous experience in Kenya as well as in other comparable jurisdictions shows a tendency for state officials to abuse such powers.[29] It is therefore advisable in the context of a future law reform process that the term 'authorised persons' be more specifically defined and limited so as to safeguard against the risk of unilateral and unchecked expansion of police powers by the minister.

4. Criminal offences and sanctions in the Cybercrimes Act: a comparative critique

The Kenyan Cybercrimes Act provides, in Part III, for the criminalisation of 27 offences. This far exceeds the number of offences in the Budapest Convention on Cybercrime,[30] which, together with its Protocol,[31] criminalises a total of 14 offences. It also surpasses the number of offences in the Malabo Convention on Cyber Security, which lists 13 offences. This greater number of offences results from splitting cybercrimes to highlight specific criminalised conduct as well as from the criminalisation of conduct relating to the fraudulent or wrongful use of electronic data. Although this approach is not without some merits, the overall impact of stipulating many offences leads to unnecessary duplication of offences.

28 Sections 48(1), 48(4), 49(2), 49(3), 50(1), 51(1), 51(7), 52(1), 53(1), 53(2) and 54(2).

29 *Law Society of Kenya v Inspector General Kenya National Police Service and 3 Others* [2015] eKLR; *Coalition for Reform and Democracy (CORD) and 2 Others v Republic of Kenya and Others* [2015] eKLR. For a comparative account on how this power has tended to be abused in other jurisdictions, see Omotubora, A. (2019) 'Old Wine in New Bottles: Critical and Comparative Perspectives on Identity Crimes under the Nigerian Cybercrime Act 2015' *African Journal of International and Comparative Law* 27(4): 609-628.

30 Clough, J. (2014) 'A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation'. *Monash University Law Review* 40(3): 698.

31 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (28 January 2003).

Unlike the Budapest Convention and the national cybercrime laws of some states,[32] the Kenyan Cybercrimes Act does not explicitly classify its offences into distinct categories of cybercrimes. In the Budapest Convention, these include (i) offences against the confidentiality, integrity and availability of computer data and systems; (ii) computer-related offences; (iii) content-related offences; and (iv) offences related to criminal infringements of copyright and other related rights (Chapter II, Section 1, Titles 1–4). Nonetheless, as with the Malabo Convention on Cyber Security, a closer review of the structure of Part III of the Kenyan Cybercrimes Act shows that the criminalised offences are arranged approximately into the four categories of cybercrime. For this reason and in the interests of brevity, the comparative analysis of the offences established in the Kenyan Cybercrimes Act is based broadly on these four types of cybercrime.

4.1 Unauthorised access

Section 14(1) of the Kenyan Cybercrimes Act criminalises unauthorised access, which entails intentional infringement of security measures with intent to gain unlawful access to a computer system, and with the knowledge that such access is unauthorised.[33] This provision is welcome to the extent that it specifies the material element of the offence that must be satisfied before criminal liability attaches: it requires the actual or attempted breach of security measures of a computer system. However, it offers no elaboration of the acts that constitute gaining or securing access. This is an omission that may present some difficulty when adjudicating alleged cybercrimes. By contrast, section 2(2)(a–d) of the South African Cybercrimes Act 2020 provides a detailed exposition of the instances in which it can accurately be alleged that a person has intentionally and unlawfully secured access to data, a computer program, a computer data storage medium and a computer system. This provides an instructive basis for amending the text of section 14(1) to strengthen its currently defective material element.

Also, the wording of the mental element of the offence of unauthorised access is inelegant, legally defective and inadequate. Although section 14(1) of the Kenyan Cybercrimes Act seems consistent with article 29(1) of the Malabo Convention on Cyber Security and article 2 of the Budapest Convention on Cybercrime, it falls short of the legal standards in these international treaty instruments.[34] In particular, it fails to specify the qualitative nature of intent as either fraudulent or dishonest, and it does not disclose the motive of such access. Section 14(3) of the Act is also defective because it distorts the relevance of intent as a core element of the crime and renders it irrelevant what the criminal motive or objective is.

32 See Clough, J. (2015) *Principles of Cybercrime.* Cambridge: Cambridge University Press.

33 'A person who causes, whether temporarily or permanently, a computer system to perform a function, by infringing security measures, with intent to gain access, and knowing such access is unauthorised, commits an offence and is liable on conviction, to a fine not exceeding five million shillings or to imprisonment for a term not exceeding three years, or to both.'

34 Jamil (2016) 'Comparative Analysis'.

A constructive method of illustrating the deficiency of section 14 of the Cybercrimes Act is to juxtapose it with an equivalent provision that is more comprehensively drafted. Article 2 of the Budapest Convention on Cybercrime criminalises illegal access to a computer system and also imposes an obligation on each of the states parties to:

> *establish as criminal offences, under its domestic law, when committed intentionally, the access to the whole or any part of the computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.*

Like section 14(1) of the Kenyan Cybercrimes Act, the above provision specifies the mental elements of the offence: it must be committed 'intentionally' and 'without right'. However, unlike section 14(1), article 2 of the Budapest Convention further specifies that the nature of the intent must be dishonest. More importantly, it draws a connection between these mental elements and the underlying criminal objective by clarifying, in inclusive language, that the ultimate motive of the illegal access should be to obtain computer data or for other dishonest ends. It is thus recommended that section 14 of the Kenyan Cybercrimes Act be amended to better clarify the specific mental elements of the dishonest intent to gain access to a computer system for the purpose of obtaining computer data, or to commit or facilitate the commission of another offence.

Despite its imperfect drafting, section 14 of the Kenyan Cybercrimes Act creditably seeks to define what constitutes 'unauthorised access'. Section 14(2)(a–b) states that access by a person to a computer system is unauthorised if that person (i) is not 'entitled to control access of the kind in question to the program or data'; or (ii) 'does not have consent from any person who is entitled to access the computer system through any function to the program or data.' This makes it easier for law enforcement and judicial authorities to distinguish between lawful and unlawful access, and is thus a laudable merit of the Kenyan Cybercrimes Act.

4.2 Access with intent to commit a further offence

Section 15(1) of the Kenyan Cybercrimes Act criminalises unauthorized access 'with intent to commit a further offence under any law, or to facilitate the commission of a further offence by that person or any other person'. Section 15(2) additionally stipulates that it is immaterial that the further offence was committed at the time when the unauthorised access was secured or at any other time. For an offence that exposes individuals upon conviction to a prison term of up to 10 years or a fine of up to Ksh 10 million, section 15 establishes a broad offence that fails to take sufficient account of the seriousness of the criminalised conduct or its temporal scope. The adverse implication here is that its penal regime does not distinguish between serious and less serious offences. This is an acute legislative flaw that calls for urgent reform.

Besides failing to criminalise only intent to commit a specific act of serious gravity, offences of the kind outlined in section 15 of the Kenyan Cybercrimes Act are not recognised in the Budapest Convention on Cybercrime or the Malabo Convention on Cyber Security. This omission may suggest that the conduct criminalised in section 15 of the Kenyan Cybercrimes Act could effectively be addressed within the offence of unauthorised access. Even so, the legislation from comparable jurisdictions indicates recognition of the need for a distinct offence of unlawful access with intent to commit specific criminalised conduct.

Although not identical in wording to the equivalent Kenyan provision, section 36 of the Nigerian Cybercrimes Act 2015 criminalises gaining access, with the intent to defraud, to any device, attachment, email or website to obtain credit card details.[35] In contrast to both the Kenyan and the Nigerian provisions, section 4 of the South African Cybercrimes Act 2020 criminalises only the unlawful and intentional securing of access. The most commendable aspect is that it crucially relates the criminalised act to other offences, including unlawful acts in respect of software (section 2(2)(c)) and the unlawful dealing in passwords, access codes or similar data or devices (sections 7(1) and 7(2)).

This suggests that the drafters of section 15 of the Kenyan Cybercrimes Act likely envisaged the types of offences described in the equivalent cybercrime laws of South Africa and Nigeria, but the text of the resulting provision falls short of the requirements of specificity and legal certainty.[36] To remedy this defect, it is proposed that section 15(1) of Kenya's Cybercrimes Act also criminalise unauthorised access that is designed or intended to facilitate a specified range of offences. Guided by the imperative of legal certainty, it is further proposed that an inclusive list of further offences to which penalty applies on conviction be enumerated in the amended provision. The cross-referencing technique used in the South African Cybercrimes Act 2020 is also highly recommended. On the same rationale, section 15(2) of Kenya's Cybercrimes Act, which makes irrelevant the gravity or timing of the offence, should be struck out altogether.

4.3 Unauthorised interference

Section 16(1) of the Kenyan Cybercrimes Act subjects any person who intentionally and without authorisation carries out any act that causes unauthorised interference to a computer system, program or data to a penalty, on conviction, of a fine not exceeding Ksh 10 million[37] or to imprisonment for a term not longer than five years, or to both. In the

35 Chakwi, M., Darwish, A., Khan, M.A. and Tyagi, S. (2015) 'Cybercrime, Digital Forensics and Jurisdiction'. *Studies in Computational Intelligence*. Springer.

36 *R v Rimmington and Goldstein* [2006] 1 AC 549, para. 33: 'There are two principles: no one should be punished under a law unless it is sufficiently clear and certain to enable him to know what conduct is forbidden before he does it; and no one should be punished for any act which was not clearly and ascertainably punishable when the act was done.'

37 Approximately US$82,045.

BAKE case, this section was the subject of a constitutionality challenge on the ground that it does not specify the element of *mens rea* and thus risks criminalising innocent conduct.[38]

Section 16(2)(a–b) of the Kenyan Cybercrimes Act defines unauthorised interference as action causing interference perpetrated by a person who (i) is 'not entitled to cause that interference' or (ii) 'does not have consent to interfere from a person who is so entitled.' In the event that unauthorised interference results in significant financial loss to any person, threatens national security, causes physical injury or death to any person or threatens public health or public safety, section 15(3) of the Act imposes much stiffer penalties on conviction: a fine not exceeding Ksh 20 million or imprisonment for a term not exceeding 10 years, or both.

While the provisions of section 16 of the Kenyan Cybercrimes Act address important aspects of cybercrime regulation, they are deficient in ways that can best be illustrated by comparison. Section 16(1) of the Act criminalises unauthorised interference without relating it to the corresponding degree of harm. This runs into the difficulty of creating a vague offence that fails to satisfy the requirement of legal certainty.[39] By contrast, article 5 of the Budapest Convention on Cybercrime, which criminalises the equivalent offence of system interference, refers to the requisite threshold of harm using the words 'serious hindering'.[40] This indicates a high level of seriousness of damage or impairment.[41] To strengthen section 16 of Kenya's Cybercrimes Act, it is proposed that its content be modified by specifying the degrees of harm outlined in section 16(3)[42] in section 16(1), and by enunciating the material element of the offence as either serious damage or impairment of the functionality of a computer system.

A suitable model to guide the amendment of section 16 of the Kenyan Cybercrimes Act is section 5 of the South African Cybercrimes Act 2020. That provision helpfully explains that interference with a computer data storage medium, a computer program or a computer system means to permanently or temporarily interrupt or impair the functionality or to render the data or computer program ineffective.

38 *BAKE v Attorney General and 3 Others* [2020] eKLR, paras 87 and 89.

39 This standard, which applies across common law jurisdictions, was clarified by the United Kingdom House of Lords in *R v Rimmington and Goldstein* [2006] 1 AC 549, para 33.

40 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.'

41 Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime*. Strasbourg: Council of Europe.

42 'A person who commits an offence under subsection (1) which – (a) results in a significant financial loss to any person; (b) threatens national security; (c) causes physical injury or death to any person; or (d) threatens public health or public safety, is liable, on conviction, to a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.'

4.4 Unauthorised interception

Section 17(1) of the Kenyan Cybercrimes Act is formulated in a manner similar to section 16(1);[43] it criminalises the conduct of a person who intentionally and without authorisation carries out any act that, directly or indirectly, intercepts or causes the interception of transmission of data to or from a computer system. In the *BAKE* case, the petitioners contended that section 17(1) of the Act created an offence without specifying the element of *mens rea* and was therefore unconstitutional.[44] Section 17(2) provides enhanced sanctions for identical offences to those in section 16(3).[45] As with section 16, the provisions of section 17 establish an unduly broad range of offences. Thus, to avoid duplication, the comments made above[46] on the need for specificity in section 16 apply in like manner to the corresponding provisions of section 17.

However, a notable aspect of unauthorised interception as set out in the Kenyan Cybercrimes Act that requires special mention is the content of the offence. Compared with international instruments on cybercrime,[47] the offence of unlawful or illegal interception is deficient and a number of crucial elements of the offence are omitted.[48] To illustrate this, it is instructive to examine the text of article 3 of the Budapest Convention on Cybercrime, which establishes the equivalent offence of illegal interception and calls for its criminalisation:

> *when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.*

These detailed provisions indicate that, as presently constituted, section 17 of the Kenyan Cybercrimes Act is incomplete and imprecise.

To remedy these shortfalls, it is recommended that section 17 of Kenya's Cybercrimes Act be amended to criminalise only the interception of 'non-public' transmissions of computer data made possible by use of 'technical means'. Also advocated is the inclusion in section 17(1) of an offence relating to electromagnetic emissions, which are not 'data' in the technical sense.[49] However, as clarified in the explanatory report to the Budapest Convention, because 'data can be reconstructed from such emissions,' the dishonest and intentional interception of data from electromagnetic emissions from a computer system should be included within the ambit of section 17(1).[50] Section 17(1) should further

43 See Section 4.3 of this article.
44 *BAKE v Attorney General and 3 Others* [2020] eKLR, paras 87 and 89.
45 See Section 4.3 of this article.
46 See Section 4.3 of this article.
47 Budapest Convention on Cybercrime article 3; Malabo Convention on Cyber Security article 29(2)(a).
48 Budapest Convention on Cybercrime article 5; Malabo Convention on Cyber Security article 29(1)(d).
49 Clough (2015) *Principles of Cybercrime*.
50 Council of Europe (2001) *Explanatory Report to the Convention on Cybercrime*, para. 57.

incorporate the *mens rea* element of dishonest intent and specify that interception must be in reference to transmission of data between one computer system linked to another. This would render sub-sections 17(2), (3) and (4) redundant and subject to removal.

The text of section 3 of the South African Cybercrimes Act 2020, which criminalises unlawful interception of data, is a suitable model on which the revision of the equivalent Kenyan provision can be based. The reason for this is that, unlike section 17 of the Kenyan Cybercrimes Act, it includes all the essential elements of the offence of unlawful or illegal interception. In addition, section 3 of the South African Cybercrimes Act 2020 aligns with the international standards in the Budapest Convention on Cybercrime.

4.5 Illegal devices and access codes

Section 18(1) of the Kenyan Cybercrimes Act envisages the criminal liability of anyone who knowingly 'manufactures, adapts, sells, procures for use, imports, offers to supply, distributes or otherwise makes available a device, program, computer password, access code or similar data' designed or primarily adapted to commit a cybercrime. Section 18(2) extends criminal liability to anyone who knowingly receives or is in possession of such illegal devices or programs as a result of, or with the intention to use it to commit, an offence under the Act. The wording of section 18(1) of Act is unsatisfactory as it uses the *mens rea* standard of 'knowingly' in relation to dynamic technologies with dual-use capabilities that can equally be used for lawful or unlawful purposes.[51]

This standard therefore unwisely criminalises an overbroad category of activities and exposes a wide range of actors (virtually the entire chain, from manufacturer, to distributor, to retailer, to end-user) to criminal liability, as all may have knowledge of the potential dual uses of such technology. This clearly highlights the pernicious implications of expansively criminalising the use of computer software and devices.[52] An analogy that can illustrate the adverse effect of section 18 of the Kenyan Cybercrimes Act may be drawn from manufacturers, wholesalers, retailers and users of glass products: while all parties know that broken glass may be used as a weapon, this does not in itself justify criminalising dealing in glassware.

A more appropriate legal standard of criminal intent should therefore be substituted for 'knowingly' in order that the criminality of illegitimate use of dual-use tools should turn exclusively on proof of the subjective intent to commit a cybercrime.[53] It is proposed that 'intentionally' is a much better-suited standard as it clearly reflects the deliberation between the actor and the crime. In its amended form, therefore, section 18 of the Kenyan Cybercrimes Act should criminalise intentional possession without justifiable cause and use of illegal devices and codes for the purpose of committing a cybercrime.

51 Day, E. and Bryant, R. (2016) 'Law and Digital Crime', in R. Bryant (ed.) *Policing Digital Crime*. Abingdon: Routledge.
52 Sommer, P. (2006) 'Criminalizing Hacking Tools'. *Digital Investigations* 3(2): 68-72.
53 Clough (2015) *Principles of Cybercrime*.

Another possible descriptor of the specific intent element of this offence may be 'unlawfully and intentionally', as used in the South African Cybercrimes Act 2020. Article 6 of the Budapest Convention on Cybercrime, which establishes the equivalent offence of misuse of devices, criminalises similar conduct when it is 'committed intentionally and without right'. The text of article 6 of the Budapest Convention, unlike that in the Malabo Convention on Cyber Security (in article 29(1)(h)), is better placed to offer a model for amending section 18(1) of the Kenyan Cybercrimes Act. Section 7 of the South African Cybercrimes Act 2020 is also an instructive basis for guiding legal reform because, unlike its Kenyan equivalent, it specifically criminalises the possession and use of computer devices and tools for purposes of committing particular prohibited acts.

It is notable that section 18(3) of the Kenyan Cybercrimes Act provides safeguards by exculpating as non-criminal a narrow set of conduct relating to the possession and use of passwords and access codes. These include any act intended for the authorised training, testing or protection of a computer system; or the use of a computer program or password or access code in compliance or accordance with a lawfully issued judicial order. This is a prudent provision that immunises a crucial component of the work of information and communication technology professionals and system administrators – testing the soundness of computer security systems, which invariably entails trying to breach firewalls.[54] A provision that draws a clear distinction between, on the one hand, legitimate and protected conduct and, on the other, illegal and punishable conduct is certainly well conceived.

Closely related to section 18 of Kenya's Cybercrimes Act is section 19, which criminalises the unauthorised disclosure of any password, access code or other means of gaining access to any program or data held in any computer system. The operative elements of this offence are that such disclosure should be made 'knowingly' and 'without authority'. Problems related to the use of 'knowingly' as a standard of specific intent have been stated above and will not be repeated.[55] As for the element of 'without authority', this presents a serious challenge to effective enforcement because it is not defined in the Kenyan Cybercrimes Act. The combined effect of these two elements is that section 19 of the Act will criminalise legitimate conduct because, unlike section 18(3), it does not immunise training, testing or protection of computer systems. Nor does it immunise other related and legitimate activities that may be facilitated by the disclosure or sharing of passwords and access codes. This is a weakness of the Kenyan Cybercrimes Act that needs to be reconsidered.

54 'Many items of this nature [i.e. passwords and access codes] are "dual use", and widely used by security professionals and system administrators. For example, penetration testing devices are used to detect security weaknesses, but may also be used by hackers as a way of gaining unauthorised access' (Clough, 2015, *Principles of Cybercrime*: p.135).

55 See Sections 4.3 and 4.4 of this article.

Some useful insight to guide the amendment of section 18 of the Kenyan Cybercrimes Act may be drawn from the South African equivalent. Section 7 of the South African Cybercrimes Act 2020 criminalises the unlawful acquisition, possession, provision, receipt or use of a password, access code or similar data. The elements of this offence in the South African Cybercrimes Act 2020 are that a person unlawfully and intentionally acquires, possesses, provides to another person or uses the password, access code or similar data for purposes of committing a cybercrime (section 7(1)). As well as clearly articulating the elements, the South Cybercrimes Act offers a basis to exculpate certain legitimate action that may constitute the offence. Section 7(2) immunises such legitimate conduct where a person found in possession of a password or access code is able to give 'a satisfactory exculpatory account of such possession'.

4.6 Offences involving a protected computer system

Section 20(1) of the Kenyan Cybercrimes Act establishes an enhanced penalty for (i) unauthorised access, (ii) access with intent to commit a further offence, (iii) unauthorised interception and (iv) unauthorised interference, where these are committed on a 'protected computer system'. Such systems are defined in section 20(2)(a–f) of the Act as those 'used directly in connection with, or necessary for' national security; protecting the existence or identity of a confidential source of information related to law enforcement; provision of services related to communication infrastructure and electronic banking or financial services; protection of public safety and emergency services; provision of national registration systems; or such other systems as may be designated by the cabinet secretary relating to information and communication technology.

These examples are imprecisely worded, with the result that the narrow category of protected computer systems may become too expansive for efficient judicial management. It therefore becomes impossible for individuals to engage in ordinary computer-related activity without the anxiety of being at risk of onerous legal liability. For this reason, among others, it is proposed that section 20(2) of the Kenyan Cybercrimes Act be amended and formulated along the lines of comparable national cybercrime laws that protect critical information infrastructure.[56] In addition, it is recommended that the words 'protected computer system' be replaced with 'critical information infrastructure', which communicates clearly the national importance of the specified computer systems and the seriousness of any attacks on them.[57]

Nigerian cybercrime law may be instructive in this regard. Section 5(1) of the Nigerian Cybercrimes Act 2015 provides, *inter alia*, that any person who intentionally commits any offence punishable under the Act against any critical national information infrastructure is liable, on conviction, to imprisonment for a term not exceeding 10 years without

56 Clough (2015) *Principles of Cybercrime*.

57 Reich, P. (2012) 'To Define or Not to Define: Law and Policy Conundrums for the Cybercrime, National Security, International Law and Military Law Communities', in P. Reich and E. Gelbstein (eds) *Law, Policy and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization*. Hershey, PA: IGI Global.

the option of a fine.[58] What is more, this Act defines 'critical national information infrastructure' as certain designated computer systems, networks, programs and traffic computer data, the destruction of which would have a debilitating impact on national security, public health and safety, or a combination of these (section 42). A more concise and better-drafted definition of critical cyber-infrastructure is found in the text of the equivalent United States legislation that inspired the Nigerian cybercrime law:

> *In this section, the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*[59]

Although the United States and Nigerian statutes do not identify precisely what constitutes critical national information infrastructure, they are instructive to the extent that both advert to a high threshold of harm – incapacitation or destruction of such critical cyber-infrastructure that can result in a 'debilitating impact'. This, unlike the position in section 20 of Kenya's Cybercrimes Act, comports with the standard of serious damage or impairment reflected in international best practice.[60] The implication here, which is simultaneously a recommendation towards amending section 20 of Kenya's Cybercrimes Act, is that only serious impairment or loss should attract the enhanced penalties.

The South African Cybercrimes Act 2020 arguably offers more precise guidance on what amounts to critical national cyber-infrastructure. Section 11 criminalises as an 'aggravated offence' interception, interference, misuse of computer data or computer system in relation to a restricted computer system. The phrase 'restricted computer system' is functionally equivalent to 'critical national infrastructure' as used in the Nigerian Cybercrimes Act, and is defined as:

> *any data, computer program, computer, computer data storage medium or computer system –*
>
> *i. under the control of, or exclusively used by –*
>
> *ii. (aa) a financial institution; or*
>
> *iii. (bb) an organ of state as set out in section 239 of the South African Constitution, including a court; and*
>
> *iv. which is protected by security measures against unauthorized access or use.*

58 Okoh, J. and Chukwueke, E. (2016) 'The Nigerian Cybercrime Act 2015 and Its Implications for Financial Institutions and Service Providers'. *Financier Worldwide*, July.

59 42 US Code § 5195c.

60 Jamil (2016) 'Comparative Analysis'.

Another aspect of the provisions for enhanced offences against protected computer systems in the Kenyan Cybercrimes Act that call for reform is the high degree of ministerial discretion. Section 20(2)(f) of the Kenyan Cybercrimes Act empowers the cabinet secretary responsible for matters relating to information, communication and technology to designate as a protected computer system in 'the manner or form as [he/she] may consider appropriate' any other computer system that he or she regards fit. The formulation of this provision establishes a broad and inexact discretion because it offers no guidance on the categories of systems that may possibly be included in the class of protected computer systems. Apart from being open to governmental abuse, this lack of guidance may diminish the heightened status of protection accorded to critical national information infrastructure.

Accordingly, it is recommended that section 20(2)(f) of the Kenyan Cybercrimes Act be amended to better define the category of protected computer systems and specify clear limits on ministerial discretion. In particular, there should be a requirement that the cabinet secretary designate, on the basis of justifiable reasons, that a particular computer system or network is crucial in protecting a vital national interest.[61] This recommendation for legislative reform coheres with the requirement in article 47 of the Kenyan Constitution to supply reasons for administrative decisions that may affect fundamental rights or other legal interests.

Commentators on the legislative antecedents of the Kenyan Cybercrimes Act observed that the provisions equivalent to section 20 of the current Act were unnecessarily duplicative and could be omitted by means of more careful legal drafting.[62] They suggested two aspects of this preferred approach. First, it was proposed that, if the intentionality requirements in sections 14, 15, 16 and 17 of the Act were heightened, the additional penalties in section 20 could be rendered redundant. Second, it was argued that, if the specification of the relevant degrees of harm were included and targeted references were made to a better defined set of critical national information infrastructure, section 20 of the Act again could be rendered unnecessary. This is a prudent approach that is in accordance with the public policy objective of having fewer yet more detailed cybercrimes. It is thus endorsed as a recommended amendment to Kenya's Cybercrimes Act.

4.7 Computer forgery and fraud

Section 25(1) of the Kenyan Cybercrimes Act criminalises the conduct of any person who 'intentionally inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible.' The text of this provision is derived, almost word for word, from article 7 of the Budapest

61 Article 19 (2018) *Kenya: Computer and Cybercrimes Bill 2017.* London: Article 19.
62 Ibid.

Convention on Cybercrime,[63] and it is also substantially the same as article 29(2)(b) of the Malabo Convention on Cyber Security.[64] However, section 25(2) of Kenya's Cybercrimes Act differs in a key respect from the equivalent provisions in these international treaties; it establishes enhanced penalties if the computer-related forgery is committed 'dishonestly or with similar intent—(a) for wrongful gain; (b) for wrongful loss to another person; or (c) for any economic benefit for oneself or for another person.'

In contrast, both the Budapest Convention on Cybercrime and the Malabo Convention on Cyber Security require as an essential element of the offence 'an intent to defraud, or similar dishonest intent, before criminal liability attaches.'[65] This indicates that section 25(2) of the Kenyan Cybercrimes Act unnecessarily creates heightened criminal sanctions for offences that should be encompassed under section 14(1) of the Act. To better serve public policy objectives and to comply with the *ultima ratio* rule of minimal criminalisation,[66] section 14(1) of the Act should be amended to incorporate 'dishonest intent' as a core element of the offence of computer-related forgery, while the fraudulent intent can be an example of such dishonesty.

Section 26(1) of the Kenyan Cybercrimes Act, which is closely related to section 25(1), criminalises computer fraud. It provides that a 'person who, with fraudulent or dishonest intent', unlawfully gains an economic benefit for himself/herself or another person, or occasions a loss to another person, through the use of a computer system, program or data, commits an offence. With appropriate adaptation, the text of section 26(1) of the Act presents a viable model for moulding the proposed changes to section 25(1) of Kenya's Cybercrimes Act.

Even so, section 26(2) of the Kenyan Cybercrimes Act is not exactly a model of clarity. Its description of the 'means' by which computer fraud may be carried out is overly complicated and long-winded when juxtaposed with the more concisely formulated equivalent provisions of the Budapest Convention on Cybercrime (article 8) and the Malabo Convention on Cyber Security (article 29(2)(d)). The latter provisions, which reflect international best practice standards, regard as sufficient that national cybercrime laws criminalise gaining of any benefit or causing loss to another person through means of any

63 'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible.'

64 'State Parties shall take the necessary legislative and/or regulatory measures to make it a criminal offence to: ... Intentionally input, alter, delete or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible.'

65 Jamil (2016) 'Comparative Analysis'.

66 Viano, E.C. (2017) 'Cybercrime: Definition, Typology, and Criminalization', in E.C. Viano (ed.) *Cybercrime, Organised Crime, and Societal Responses: International Approaches*. Amsterdam: Springer.

interference with the functioning of a computer system. Thus it is recommended that section 26 be simplified to bring it in line with article 29(2)(d) of the Malabo Convention on Cyber Security and article 8 of the Budapest Convention on Cybercrime.

4.8 Cyber-harassment

Section 27(1) of Kenya's Cybercrimes Act criminalises cyber-harassment and is one of the provisions whose constitutionality was challenged in the *BAKE* case.[67] The *BAKE* petitioners submitted that section 27 criminalised speech on grounds that had no proximate relationship to the legitimate grounds for limitation of free speech;[68] and further, that in doing so, it used vague and subjective phrases such as 'apprehension of fear or violence' and 'indecent or grossly offensive'.[69] The offence of cyber-harassment is described in section 27(1) of the Act as consisting in the action of:

> *A person who, individually or with other persons, wilfully communicates, either directly or indirectly, with another person or anyone known to that person … 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.*

This definition is problematic for two reasons. First, it is unduly complex, legally imprecise and, in turn, unclear in its meaning. It is notable, however, that the effects specified in clauses (a) and (b) of section 27(1) of the Kenyan Cybercrimes Act reflect the threshold test of harm articulated by the House of Lords in *Chambers v Director of Public Prosecutions (DPP)*.[70] In that case the lord chief justice held that 'a message which does not create fear or apprehension in those to whom it is communicated, or may reasonably be expected to see it, falls outside [the criminalized conduct] for the simple reason that the message lacks menace' (para. 30). To this extent, section 27(1) partially meets the best international practice standards. Still, despite the well-conceived elaboration of the harm caused by cyber-harassment in clauses (a) and (b), the prolix introductory sentence makes it difficult to ascertain the actions that are criminalised.

67 *BAKE v Attorney General and 3 Others* [2020] eKLR, para. 73.

68 Constitution of Kenya, article 33(2): 'The right to freedom of expression does not extend to—(a) Propaganda for war; (b) Incitement to violence; (c) Hate speech; or (d) Advocacy of hatred that—(i) Constitutes ethnic incitement, vilification of others or incitement to cause harm; or (ii) Is based on any ground of discrimination specified or contemplated in Article 27(4).'

69 *BAKE v Attorney General and 3 Others* [2020] eKLR, para. 73.

70 [2012] EWHC 2157 (Admin) (QB).

Other critical elements, such as what would constitute harassment or the repetitive nature of the offensive cyber-conduct, are not clarified in section 27(1) of Kenya's Cybercrimes Act.[71] The case law from the United Kingdom may offer useful guidance on this point. In *Jones v DPP,* the legal elements used to establish the offence of cyber-harassment were expounded in a concise way.[72] It was held that (i) the impugned conduct must form part of a sequence of connected acts, but each individual act forming part of the sequence need not be of sufficient gravity to be a crime in itself; (ii) the sequence of acts or course of conduct must involve incidents on at least two occasions and must not be two temporally distant incidents; and (iii) the fewer the incidents, the more serious its gravity should be to amount to harassment.

In this connection, two observations can be made regarding section 27(1) of the Kenyan Cybercrimes Act. First, it falls short of the required legal standards of certainty and should be amended to reflect this general principle of law.[73] Second, it conflates two distinct concepts – cyberstalking and cyberbullying – which should ideally be categorised as separate offences.[74]

It is noteworthy that neither the Budapest Convention on Cybercrime nor the Malabo Convention on Cyber Security have provisions for cyberstalking and cyberbullying. On one view, this may suggest that their constitutive conduct is not regarded as fit for criminal regulation. Indeed, comments on similar provisions in earlier legislative drafts of Kenya's Cybercrimes Act indicated that cybercrime or cybersecurity legislation was not an appropriate venue for addressing state failure to protect individuals from harassment, threats and other forms of intimidation.[75] This reflects the view that favours self-regulation of the Internet rather than regulation by way of prescriptive legislation.[76] It also fits with the principle of minimal criminalisation of cyber-conduct on the rationale that what is illegal offline is likewise illegal online.[77]

However, the central role that information and communication technology has come to play in social interactions and its prodigal capacity for facilitating criminal conduct may justify inclusion in national law of offences against cyberstalking and cyberbullying.[78] Indeed, some Commonwealth jurisdictions, such as Canada, New Zealand[79] and the United Kingdom,[80] have been persuaded to establish a regulatory framework

71 Sugow, A., Zalo, M. and Rutenberg, I. (2021) 'Appraising the Impact of Kenya's Cyber-Harassment Law on the Freedom of Expression'. *Journal of Intellectual Property and Information Technology Law* 1(1).
72 [2015] 1 WLR 833.
73 *R v Rimmington and Goldstein* [2006] 1 AC 549, para. 33.
74 *Wilson v R* [2012] VSCA 40.
75 Article 19 (2018) *Kenya: Computer and Cybercrimes Bill 2017.*
76 UK Government (2017) *A Safe and Secure Cyberspace – Making the UK the Safest Place in the World to Live and Work Online*.
77 Criminal Code of Canada, section 243.
78 Clough, J. (2014) 'A World of Difference'.
79 Harmful Digital Communications Act 2015.
80 Criminal Justice and Courts Act 2015, section 33; Malicious Communications Act 1988, section 1; Protection from Harassment Act 1997, sections 2A and 4A; Communications Act 2003, section 127.

to legally regulate online abusive behaviour. Their laws criminalise various forms of online harassment and bullying, including trolling, doxxing, identity theft and revenge pornography.[81] The guidance issued by the United Kingdom Crown Prosecution Service[82] relating to the effective prosecution of, among other crimes, cyberbullying and online harassment provides a reasoned basis for criminalising the conduct described in section 16(1) of the Kenyan Cybercrimes Act.

In addition, comparable cybercrime law from New Zealand can offer a suitable model for proposed amendments to section 27(1) of Kenya's Cybercrimes Act, as well as to other sectoral laws in Kenya. Section 6 of New Zealand's Harmful Digital Communications Act 2015 establishes 10 communications principles, including that digital communication should not be threatening, intimidating or menacing; incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual; be used to harass an individual; incite or encourage an individual to commit suicide; disclose sensitive personal facts about an individual; be grossly offensive to a reasonable person in the position of the affected individual; and be indecent or obscene.

These prohibited actions better illustrate some of the effects of the conduct criminalised in section 27(1) of the Kenyan Cybercrimes Act. Moreover, section 22(1) of the New Zealand Act defines the types of online and computer-related acts that may constitute the offence of causing harm by posting digital communication, and section 22(2) further specifies the relevant factors that should be considered by a court in 'determining whether a post would cause harm'.

Elements of the offence of cyber-harassment as specified in section 27(1) of the Kenyan Cybercrimes Act are inconsistent with the general principles of criminal law. The section does not specify the nature of the criminal intent as either fraudulent or malicious. Also, although it emphasises recurrence, it renders irrelevant the requirement of reasonable direct foreseeability of harm requirement. This may result in the criminalisation of possible erroneous actions that have no malicious intent.[83] In addition, the language used to describe the effects of the offence is vague and overbroad. It may be more constructive to require that the harm be not merely apprehended but also satisfy a higher and more definite threshold.

The comparable national cybercrime laws cited above adopt the legal standard of real or substantial risk. These are useful pointers for the reform of section 27 of Kenya's Cybercrimes Act. Also, as required under section 103 of the United Kingdom's Digital Economy Act 2017, it may be prudent to recommend that the cabinet secretary issue guidance to social media providers on actions that may be appropriate to take against online bullying, intimidation or humiliation.

81 Strickland, P. and Dent, J. (2017) 'Online Harassment and Cyber Bullying'. Briefing Paper 07967. London: House of Commons Library.

82 UK Crown Prosecution Service (2018) *Legal Guidance on Stalking and Harassment*.

83 Herring, J. (2014) *Criminal Law: Text, Cases, Materials*. Oxford: Oxford University Press.

Besides an indeterminate definition of cyber-harassment in section 27(1) of the Kenyan Cybercrimes Act, the penalty for cyberstalking and cyberbullying is also questionable. Section 27(2) of the Act prescribes that, on conviction for this offence, the guilty party is liable to 'a fine not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years, or to both.'[84] This sanction is excessive and unjustified. It must be borne in mind that the acts that this offence encompasses frequently occur in the context of social relations and are a product of its breakdown.[85] Accordingly, draconian law and punitive sanctions may not be an appropriate response to this social issue.[86]

Consider the case of *A M v Premier Academy*, which was decided before the enactment of the Kenyan Cybercrimes Act.[87] The brief facts of the case are that a child was suspended from school on account of bullying other students by means of a social media network. Had section 27 of Kenya's Cybercrimes Act been in force, that child may have risked far more than just mere suspension from school: a steep fine and significant prison time. Another real risked posed by the provisions of section 27 is its potential abuse by governmental authorities to target activists and investigative journalists who routinely criticise public officials and expose their unlawful and risqué transgressions. This risk has already materialised, as illustrated by the case of *Republic v Robert Alai*.[88] In this case, a blogger who criticised the president on his Facebook page challenged the constitutionality of the decision to charge him.

4.9 Ancillary criminal law provisions

Section 46 of the Kenyan Cybercrimes Act outlines an ancillary criminal law provision to supplement the existing law by adding an enhanced penal regime if an offence is committed by cyber means. It stipulates that 'A person who commits an offence under any other law through the use of a computer system commits an offence and shall be liable on conviction to a penalty similar to the penalty provided under that law.' The effect of section 46 of the Act is to impose on an already established sentencing regime a mandatory requirement that judicial officers should add significant penalties for the mere reason that an offence was committed through the use of a computer system. This provision is inappropriate for at least two reasons.

First, it results in the duplication of legislative effort because the Kenyan Cybercrimes Act criminalises a broad range of offences that effectively encompass conduct for which section 46 of the Act seeks to impose an additional penalty. These offences can be categorised as including (i) offences against the confidentiality, integrity and availability of

84 The amount of Ksh 10 million is approximately US$82,045.
85 BAKE (2018) *State of the Internet in Kenya 2017*.
86 Brenner, S. (2007) 'Cybercrime: Re-thinking Crime Control Strategies', in Y. Jewkes (ed.) *Crime Online*. Cullompton: Willan Publishing.
87 [2017] eKLR.
88 [2017] eKLR.

computer data and systems; (ii) computer-related offences; (iii) content-related offences; (iv) offences related to the breach of copyright or related rights; and (v) privacy and data protection offences.

Additionally, most of the offences outlined in the Act attract substantial fines, ranging between not more than Ksh 5 million[89] and Ksh 20 million,[90] and prison terms ranging between sentences not exceeding three years and ten years. There is also the possibility of getting a fine and a prison sentence. Moreover, the majority of serious offences that may be committed by cyber means are already criminalised in the Penal Code and in specialist statutes. When considered cumulatively, it is clear that section 46 of Kenya's Cybercrimes Act is not consistent with the legal principle of minimal criminalisation, and it is also unclear what public policy aims its draconian approach would serve.

Second, section 46 of Kenya's Cybercrimes Act fails to satisfy the imperative of legal certainty.[91] Its scope is both imprecise and overbroad because it ambiguously refers to offences under any law committed through the use of a computer system. Yet it does not specify the unlawful act, nor make clear the manner in which the use of a computer system will expose one to criminal liability. This indefinite wording invariably makes the targeted criminal conduct indeterminate, and this means the section runs the added difficulty of being open to abuse.

5. Conclusion

This article has demonstrated that, while the Kenyan Cybercrimes Act is a creditable legislative step towards the end of tackling cybercrimes in Kenya, some of its provisions raise serious concerns that need to be addressed by way of amendment. Although the notable merits of the Act are no less important, the overriding interest of providing meaningful guideposts on points for reform dictate that its shortfalls be restated first, followed by the proposed corrective steps that must be taken to ensure that the Act is both effective and constitutionally compliant. Accordingly, by way of summary of the points raised and concluding observations, below is a non-exhaustive scorecard of the Kenyan Cybercrimes Act.

With reference to certain provisions discussed above,[92] the Kenyan Cybercrimes Act adopts a punitive and slipshod approach to drafting criminal offences. It has embraced such an excess of zeal in criminalising actions that it overlooks the duplication of offences.[93] With a few notable exceptions, the Act gives insufficient attention to the imperative of legal certainty by failing to specify the key elements of specific intent and the degree of harm.[94] In addition, it ardently adopts exacting sentences and onerous fines

89 Approximately US$41,022.
90 Approximately US$164,090.
91 *R v Rimmington and Goldstein* [2006] 1 AC 549, para. 33.
92 See Sections 4.3 and 4.4 of this article.
93 See sections 6, 7 and 10.
94 See Section 4 of this article.

but shows little attention to the proportionality of the sentence *vis-à-vis* the gravity of the crime or the public policy objects that are to be served by the respective sanctions. Most problematic of all, Kenya's Cybercrimes Act insidiously expands the scope of ever-greater governmental restriction on fundamental human rights, particularly when its provisions are read together with the Security Laws (Amendment) Act 2014.[95]

Despite its shortcomings, some consolation may be found in the fact that there is still an opportunity to rectify by statutory amendment the legitimation of these elements of bad law in the Kenyan Cybercrimes Act. Better still, there are specific ways by means of which this important task may be accomplished. First, there is a need for more inclusive stakeholder engagement with the Kenyan Cybercrimes Act. Thus far, public participation in the legislative and subsequent implementation processes has been modest and superficial. There has also been a marked absence of youth participation in these processes, whereas this is the demographic group that the provisions of the Act are most likely to affect.

Second, there is an urgent need to reconsider and redraft the criminal offences section so as to remove some duplicative provisions, to clearly delimit the scope of the offences and to better specify the objective and subjective elements of crime. As discussed in this article in relation to specific offences, a number of provisions overlap with or are essentially the same as others.[96] With more judicious drafting, the number of offences can be reduced, with some duplicative offences being removed altogether.

Third, the needlessly punitive regime of sentences in Kenya's Cybercrimes Act needs to be abandoned and replaced with a more context-sensitive and proportionate approach. Towards this end, it may be useful for lawmakers to have regard to the Sentencing Guidelines adopted by the Judiciary in 2015,[97] as well as to case law from the Supreme Court of Kenya.[98] Also, most of the sanctions in the Kenyan Cybercrimes Act do not draw a distinction between serious and less serious types of harm. This makes it possible for an individual guilty of cyber-conduct causing a small degree of harm to receive punishment similar to that facing another whose action results in more serious damage. Nor do the sanctions in the Act specify that only offences with criminal or dishonest or fraudulent intent attract the heavy penalties. For these, among other, reasons, the sanctions regime in the Kenyan Cybercrimes Act needs to be reformed systematically.

95 *Law Society of Kenya v Attorney General and Another; National Commission for Human Rights and Another (Interested Parties)* [2020] eKLR; *Okiya Omtatah Okoiti and 2 Others v Cabinet Secretary, Ministry of Health and 2 Others; Kenya National Commission on Human Rights (Interested Party)* [2020] eKLR.

96 See Section 4.7 of this article.

97 Judicial Service Act, Sentencing Guidelines, 2016 Gazette Notice No. 2970 of 29 April 2016.

98 *Francis Karioko Muruatetu and Another v Republic* [2017] eKLR.