ARTICLE 19

Kenya: Computer and Cybercrimes Bill

September 2016

Legal analysis

Executive summary

In September 2016, ARTICLE 19 reviewed the draft Computer and Cybercrimes Bill, 2016 (Draft Cyber-crimes Bill), currently being discussed in Kenya, for its compliance with international freedom of expression standards. This is the second review of this piece of legislation as in July 2014, we analysed the first draft of this legislation (Cybercrime and Computer related Crimes Bill).

Our analysis shows that the Draft Cybercrimes Bill contains several important additions that are apparently modelled after relevant international standards. ARTICLE 19 notices and looks upon this positively. However, we also note that the Draft Bill also contains several broadly defined offences with harsh sentences that could dramatically chill freedom of expression online in Kenya. Further, many of the offences unnecessarily overlap with one another.

We recommend including more precise intent and harm requirements for existing offences, namely by requiring "dishonest" intent and "serious" harm to result for most sanctions. We suggest in multiple cases a 'public interest' defence. The defence entails providing an opportunity for an accused to establish that there was no harm or risk of harm to a legitimate interest in engaging in the proscribed activity, and that the public benefit in the activity outweighed any harm.

Finally, content-based offences such as the provisions criminalising cyber-stalking and cyber-bullying fall well below international standards. We recommend entirely omitting several offences that are so broadly defined as to expose them to abuse for less legitimate ends.

Summary of recommendations:

- The Cybercrimes Bill should provide sufficient safeguards for the protection of human rights and specifically reference international standards;
- Offences included in the Bill should clearly include requirements for "dishonest" intent for their commission as well as for "serious" harm to result before criminal liability attaches;
- Public interest defences should be made available to ensure that legitimate whistleblowers acting in good faith are not prosecuted under the Bill.
- The Cybercrimes Bill should contain a definition of "damage" which requires the word "serious" impairment or losses. The definition of "computer system" should closely follow the definition contained in Article 1 of the Cybercrime Convention of the Council of Europe. In particular, the definition of computer system should make explicit reference to "automatic processing of data;"
- Section 4(1) should require either "dishonest intent to gain access", or "intent to obtain computer data;"
- Section 5(1) should remove the reference to "a further offence" and instead require specific and serious offences;
- Several provisions of the Draft Bill should be removed in their entirety, in particular Sections 4(3), 5(2), 6(3), 7(2) - 7(4), 8(2), 9, 14, 19 should be stricken out entirely.
- Section 6(1) should be amended to require serious damage or impairment;
- Section 7(1) should be brought more closely in line with Article 3 of the Cybercrime Convention, namely, it should punish the interception of "non-public" transmission of data, require interception by "technical means", and require "dishonest intent";

- "Knowingly" should be replaced with "intentionally" in Section 8(1);
- Serious consideration should be given to removing Section 10, which may be rendered unnecessary when heightened intentionality requirements and requisite "serious" harm are added to Sections 4 through 7 of the Cybercrimes Bill;
- If kept, the penalties under Section 10 should be reduced significantly;
- If kept, Section 10(1) should require the commission of the offence cause "serious" harm to a protected computer system; and
- If kept, Section 10(2)(f), allowing the Cabinet Secretary to designate protected systems at will, should have clear limitations defined in law.
- Sections 12 and 13 should be checked to ensure consistency with existing offences in the Kenyan criminal law as to avoid duplication of offline criminal conduct;
- Section 12(1) should require "dishonest" intent, and Section 12(2) should be stricken entirely; and
- Section 13 punishing computer-related fraud should be redrafted to be more consistent with Article 8 of the Cybercrime Convention. Specifically, Section 13(2) should be simplified to entail "any input, alteration, deletion or suppression of computer data" and "any interference with the functioning of a computer system;"
- Subsections 21(3)(d) through 21(3)(f) allowing for investigative orders compelling technical assistance and decryption should be amended to specify that such orders can only be obtained when they are necessary, the least intrusive means available, and focused on a specific target.

Table of contents

Introduction

In this document, ARTICLE 19 analyses the 2016 Computer and Cybercrimes Bill (Draft Cybercrimes Bill) for its compliance with international human rights standards. This is the second time that we review this type of legislation in Kenya as in July 2014, we analysed the first draft of the Cybercrime and Computer related Crimes Bill. [1] The Draft Cybercrimes Bill is the final version of the Inter-Agency technical committee where ARTICLE 19 Eastern African was a member. The Bill is now available for public review and input before it is submitted to the National Assembly.

This analysis is also conducted simultaneously with the review of the July 2016 draft of the Cyber Security and Protection Bill (Cyber-Security Bill) which is provided in a separate document.

Our analysis is based on international standards on freedom of expression, and particularly on international standards that are applicable to digital technologies. The overview of these standards has been provided in the July 2014 analysis of the first draft bill, hence we refer to the respective section of our earlier documents.

ARTICLE 19 focuses only on specific sections that raise key freedom of expression concerns. The fact that there are no comments on certain sections does not constitute their automatic endorsement by ARTICLE 19. In the The analysis not only highlights concerns and conflicts with international human rights standards within the Bill but also actively seeks to offer constructive recommendations on how the Bill can be improved. We explain the ways in which problematic provisions in the Bill can be made compatible with international standards on freedom of expression and privacy and set out key recommendations at the end of each section.

ARTICLE 19 hope that the shortcomings identified in this analysis will be addressed by its drafters before the submission of the Bill to the Parliament. We stand ready to provide further assistance in bringing it into full compliance with international standards on freedom of expression.

[1] See, ARTICLE 19, Kenya: Cybercrime and Computer Related Crimes Bill, 14 August 2014.

Analysis of the Draft Cybercrimes Bill

General Comments

Before laying down our specific concerns, ARTICLE 19 would like to make several general comments about the Cybercrimes Bill.

- **High number of offences, including overlapping offences:** We note that the Cybercrimes Bill introduces an unusually high number of computer-related offences and we question the necessity of this approach. Many of these offences overlap with or are duplicative with others in the Bill. From a comparative perspective, the Kenya legislators should consider that the CoE Cybercrime Convention contains only five such offences; whilst the UK Computer Misuse Act 1990 contains four such offences and to our knowledge there have been no concerns raised that the UK is not properly equipped to deal with cybercrime.[2] In our view, and as detailed further below, several all the offences provided for under the Cybercrimes Bill could be either regrouped and simplified or entirely removed.

- **Disproportionate sanctions:** We are concerned that the offences contained in the draft Cybercrimes Bill provide for unduly harsh sentences, including lengthy imprisonment. Moreover, most of the offences do not articulate a significant *mens rea* requirement of "dishonest" intent or the need for "serious" harm to flow from the offence before criminal liability attaches. We would therefore recommend that the sentences available for offences against the confidentiality, integrity and availability of computer data and systems should be reduced to one-year maximum.[3] In addition, a harm test or 'public interest defence' is not provided in the Bill where appropriate.

- **Lack of procedural safeguards for human rights protections:** Procedural safeguards for human rights protections are markedly absent throughout the Draft Cybercrimes Bill. There is no reference to Kenya's obligations to uphold and protect the right to freedom of expression and other human rights protected by international law.

Recommendations:

- Offences should clearly include requirements for "dishonest" intent for their commission as well as for "serious" harm to result before criminal liability attaches;
- The Cybercrimes Bill should provide sufficient safeguards for the protection of human rights and specifically reference international standards; and
- Public interest defences should be made available to ensure that legitimate whistleblowers acting in good faith are not prosecuted under the Bill.

Definitions

In general, ARTICLE 19 welcomes that this section sheds some light upon key operative

[2] The UK Computer Misuse Act 1990 ("1990 Act") proscribes unauthorised access to computer material, unauthorised access with intent to commit an offence, unauthorised access with intent to impair a computer, and making or supplying articles to commit one of the aforementioned offences.
[3] *C.f.* 1990 Act 3(6).

terms. In particular, we note that the definition of traffic data is consistent with the definition contained in the Council of Europe Cybercrime Convention (CoE Cybercrime Convention) which is an important comparative standard. [4] It is positive that Part I of the Cybercrimes Bill contains several important definitions, including "digital communication", "traffic data" "computer system", "unlawful interception" and "program."

ARTICLE 19 is concerned about the lack of definitions of some key terms connected to the prosecution of computer-related crimes, in particular:

- The Draft Bill does not provide a definition of "damage" or clarify that only "serious" impairment or losses should attract criminal sanctions;

- The Cabinet Secretary has broad discretion to expand the definition of "authorised person" under the Investigative Procedures section. This provision potentially allows for broad expansions of police powers; and

- The definition of "computer system" does not appear intrinsically problematic; we note that it fails to include a reference to "automatic processing of data" which is a key component of the definition of computer systems in the Cybercrime Convention.

Recommendations:

- The Cybercrimes Bill should contain a definition of "damage" which requires the word "serious" impairment or losses;
- The definition of "computer system" should closely follow the definition contained in Article 1 of the CoE Cybercrime Convention. In particular, the definition of computer system should make explicit reference to "automatic processing of data."

Unauthorised access

Section 4 of the Draft Cybercrimes Bill criminalises infringing security measures of computer system, with intent to gain access, and knowing that access is unauthorised. Section 4(2) defines "unauthorised" access as both not being entitled to control access, and not possessing consent from any person who is entitled to have such access.

ARTICLE 19 appreciates that Section 4 requires security features to be infringed as an element of the offence, and makes an effort to specifically define and limit what "unauthorised" access entails. These efforts are consistent with the CoE Cybercrime Convention.

However, the intentionality requirements fall short of international standards. Section 4(1) should also specify that intent to gain access be "dishonest" or that there be intent to obtain computer data. Section 4(3) is thus problematic from a perspective of intentionality because it makes immaterial whether access is directed at any particular data.

Recommendations:

- Section 4(1) should require either "dishonest intent to gain access", or "intent to obtain computer data;" and
- Section 4(3) should be stricken in its entirety.

[4] The Council of Europe Convention on Cybercrime, CETS No. 185, in force since July 2004. As of May 2015, 46 states have ratified the Convention and a further eight states have signed the Convention but have not ratified it.

Access with intent to commit or facilitate further offence, and offences committed through the use of a computer system

Section 5 of the Draft Cybercrimes Bill punishes with a sentence of up to ten years any individual violating Section 4 who intends to commit any "further offence" by that person or another person, regardless of the offence's seriousness or timing. Similarly, Section 19 punishes a person with up to four years imprisonment for committing an offence "under any other law" through the use of a computer system.

ARTICLE 19 notes that these offences do not appear in other relevant conventions, raises two primary concerns with respect to these offences:

- First, we believe that both Sections 5 and 19 fail to comply with the requirements of legal certainty under international law. The criminal law should only criminalise intent to commit both specific and serious offences rather than broadly refer to every possible offence, however minor.

  Accordingly, we recommend that the offence created by section 5(1) should be significantly narrowed. In particular, it should be made clear that unauthorised access serves as the means to or preparatory act to the commission of a further offence, which should be clearly defined.

- *Second*, we questions the necessity of the offences in Sections 5 and 19 given that the Cybercrimes Bill already criminalises unauthorised access in Section 4, and other forms of computer-related conduct in other sections. Most substantive offences that may be committed by means of computer systems, such as bank robbery, would presumably be covered already under the Kenyan criminal code or relevant statutes.

  Section 19 is even more problematic because it goes even further than Section 5, requiring only the use of a computer, without defining what or how the computer is used. A literal reading of the statute would seem to criminalise the planning of a crime via electronic mail, or the physical assault of an individual using a computer. As the existing Cybercrimes Bill provisions already address computer-related crimes, and other offences are presumably covered already under the Kenyan criminal code or relevant statutes, there is no need for this Section in the Bill.

Recommendations:
- Section 5(1) should remove the reference to "a further offence" and instead require specific and serious offences;
- Sections 5(2) and 19 should be stricken out entirely.

Unauthorised interference and interception

Section 6 of the Draft Cybercrimes Bill punishes causing interference with a computer system without authorisation, with authorisation being defined as either being entitled to cause interference, or having consent from an individual so entitled. Section 6(3) provides for heightened sanctions of up to ten years where the offence causes certain categories of proscribed harm.

ARTICLE 19 is concerned that Section 6(1) is overbroad because it punishes interference in the absence of serious damage or impairment to a computer system. From a comparative perspective, we note that Section 5 of the CoE Cybercrime Convention includes the language "serious hindering without right." The heightened offence in 6(3) enumerates several categories of harm but provides for unduly severe penalties. The categories of harm could be moved to Section 6(1) to make that provision more specific, and 6(3) would then be unnecessary.

Section 7(1) of the Draft Cybercrimes Bill punishes the interception, by "any act", of the transmission of data to or from a computer system. Section 7(2) provides for heightened sanctions of up to ten years imprisonment for specific types of harm. Sections 7(3) and 7(4) unnecessarily broaden the scope of the offence.

ARTICLE 19 notes that Article 3 of the CoE Cybercrime Convention (which punishes illegal interception) has several components not present in Section 7(1) of the Cybercrimes Bill as currently drafted. The Convention requires the interception "by technical means" of "non-public" data. As written, Section 7(1) could criminalise the interception of public data and thus should be amended to include the aforementioned terms.

Recommendations:

- Section 6(1) should be amended to require serious damage or impairment;
- Section 6(3) should be removed in its entirety;
- Section 7(1) should be brought more closely in line with Article 3 of the Cybercrime Convention, namely, it should punish the interception of "non-public" transmission of data, require interception by "technical means", and require "dishonest intent"; and
- Sections 7(2), 7(3) and 7(4) should be omitted.

Illegal devices and access codes

Section 8 of the Draft Cybercrimes Bill punishes anyone who knowingly manufactures, adapts, sells, procures, imports or distributes devices or programs adapted primarily for the purpose of committing an offence under the Bill. Section 8(2) specifically criminalises anyone who knowingly receives or is in possession of such devices or programs without justification.

ARTICLE 19 appreciates the inclusion of Subsection 8(3)(a) which prevents training, testing, or protection of computer systems from being criminalised under the provision. However, we are concerned about the current text of Section 8 for the following main reasons:

- The *mens rea* for under Section 8(1) is "knowingly" rather than "intentionally". We note that like many tools, technologies are dual-use and it is in the nature of technology that it can be used both for legitimate and illegitimate purposes. Most companies would know that the software they manufacture or sell could be used for dual purposes, including for the purposes of unauthorised access to computer data and systems. A higher standard of intent should be introduced so that "intentionally" is required in section 8(1). This is the same standard as required under Article 6 of the CoE Cybercrime Convention.

- Additionally, this provision may be used to prosecute individuals or companies producing, distributing, selling or otherwise circulating software used to break Digital Management Rights systems. DRM systems are a type of technology principally used by hardware manufacturers, publishers and copyright holders to control how digital content may be

used after sale. DRM systems are controversial from a freedom of expression perspective, as the legitimacy of copyright holders exercising in perpetuity absolute control over the sharing of information is strongly contested. For example, DRM systems prevent individuals from engaging in trivial and non-commercial acts of copyright infringement such as transferring data between their own electronic devices; they can also prevent individuals from using copyrighted works in a way that is ordinarily protected by the defence of "fair use".

Finally, we are also concerned about the scope of Section 9 of the Draft Cybercrimes Bill which criminalises anyone who knowingly discloses a password or access code without authority. The phrase "without authority" is nowhere defined, and the intentionality requirement of "knowingly" is not as protective as a heightened standard of "intentionality". The provision could therefore criminalise a number of legitimate activities such as security testing and research or the sharing of passwords for academic and personal use.

Recommendations:
- "Knowingly" should be replaced with "intentionally" in Section 8(1);
- Section 8(2) and 9 should be omitted in their entirety.

Enhanced penalty offences involving protected computer systems

Section 10 of the Draft Cybercrimes Bill provides for severe penalties for the commission of offences that are committed on protected computer systems. While Section 10(2) defines several examples of such systems, ARTICLE 19 is very concerned that these terms are broad and not formulated with sufficient precision to enable an individual to regulate his or her conduct. We believe that only "serious" impairment or losses should face criminal sanction. This reading is consistent with international standards, including the CoE Cybercrime Convention.

Moreover, adding heightened intentionality requirements to the prerequisite offences may render this provision unnecessary. The penalty of up to twenty years imprisonment is unduly severe.

Additionally, the definition of protected system is broad, most problematically in Section 10(2)(f) which affords the Cabinet Secretary unlimited discretion to designate protected computer systems as the Secretary "may consider appropriate". There is no requirement that the systems be necessary to protect any vital interest.

Recommendations:
- Serious consideration should be given to removing Section 10, which may be rendered unnecessary when heightened intentionality requirements and requisite "serious" harm are added to Sections 4 through 7 of the Cybercrimes Bill;
- If kept, the penalties under Section 10 should be reduced significantly;
- If kept, Section 10(1) should require the commission of the offence cause "serious" harm to a protected computer system; and
- If kept, Section 10(2)(f), allowing the Cabinet Secretary to designate protected systems at will, should have clear limitations defined in law.

"Child pornography"

In our comments to the provisions on "child pornography" in an accompanying analysis of the draft Cyber-security and Protection Bill, we highlight the appropriate regulation of this topic in the Kenyan legislation. We reiterate our concerns here and recommend that the issue of child sexual exploitation should be addressed in general criminal legislation.

Computer forgery and fraud

Section 12(1) of the Draft Cybercrimes Bill criminalises the intentional input or alteration of inauthentic computer data with the intent that it be acted upon for legal purposes. Section 13 punishes gaining a benefit or causing a loss via the unauthorised use of a computer system and dishonest intent.

ARTICLE 19 notes that both offences—apart from some issues enumerated below—are generally consistent with the Cybercrime Convention. However we are concerned that Sections 12 and 13 criminalise behavior using a computer that is already criminalised offline, namely forgery and fraud. We would encourage the Kenyan government to ensure consistency with existing laws covering this type of criminal conduct so as to avoid duplication.

ARTICLE 19 is also concerned that Section 12(2) attaches heightened penalties for "dishonest" intent, while the Cybercrime Convention suggests dishonest intent as a foundation for criminal liability. We would therefore recommend moving the "dishonest" intent requirement to Section 12(1) and omitting Section 12(2) in its entirety.

Section 13(2) as written is unduly complex and should be simplified in accordance with Article 8 of the Cybercrime Convention. Specifically, it suffices to proscribe "any input, alteration, deletion or suppression of computer data" and "any interference with the functioning of a computer system" with dishonest intent for the purpose of procuring an economic benefit without right.

Recommendations:

- Sections 12 and 13 should be checked to ensure consistency with existing offences in the Kenyan criminal law as to avoid duplication of offline criminal conduct;
- Section 12(1) should require "dishonest" intent, and Section 12(2) should be stricken entirely; and
- Section 13 punishing computer-related fraud should be redrafted to be more consistent with Article 8 of the CoE Cybercrime Convention. Specifically, Section 13(2) should be simplified to entail "any input, alteration, deletion or suppression of computer data" and "any interference with the functioning of a computer system".

Cyber-stalking and cyber-bullying

ARTICLE 19 is deeply concerned that Section 14, criminalizing "cyber-stalking" and "cyber-bullying", is vague and overbroad and fails to comply with requirements of legal certainty under international human rights law.

In our analysis of the Cyber Security and Protection Bill that contains similar provisions as

Section 14, we noted that State can and should protect individuals from harassment, threats and other forms of intimidation. To the extent that Kenyan law fails to provide sufficient protection in this area, the legislature should take immediate steps to ensure that the criminal law is adequate and fit for the purpose. We do not thing that specific cyber-crime or cyber-security legislation is inappropriate venue for addressing the issue. Moreover, the definition of Section 14 is not clearly limited to digital conduct; even if it were, such a limitation would fail to do enough to address problems of stalking.

ARTICLE 19 is concerned that Section 14 of the Cybercrimes Bill represents a harshly punitive attempt to address problems related to stalking and harassment. At the same time Section 14 fails to provide sufficient safeguards against misuse, particularly for legitimate protests and investigative journalism.

The intentionality terms of Section 14 are undefined, including "wilfully and repeatedly communicates", "indirectly", and "if they know or ought to know". The punishment of communication without any apparent negative intent requirement threatens to punish benign contact.

The harms are also unclear, attaching penalties of up to ten years imprisonment for causing "apprehension or fear of violence", or detrimental effects. These harms do not have to be real or even substantial, opening them up to abuse. For example, terms may be cited by government officials being contacted repeatedly by investigative journalists so long as the officials claim that the contact caused them detriment or apprehension.

While ARTICLE 19 acknowledges that Section 14(3)(c) makes a public interest defence available "in particular circumstances", we do not view that it is sufficiently articulated or protective of legitimate expression to remedy the vague terms of the offence.

Recommendations:

- Section 14 should be struck in its entirety. Legislation against stalking and harassment should be addressed by the general criminal law, rather than by cybercrime legislation. Further, such legislation must carefully articulate intentionality requirements, define substantial harms from conduct, and make available a public interest defence.

Procedures and investigations and legal assistance

The remaining sections of the Cybercrimes Bill set out investigatory powers and procedures. ARTICLE 19 does not propose to conduct an exhaustive analysis of this part of the Bill, but we do make some important observations for the protection of the rights to privacy and freedom of expression.

Duty to assist inspection or investigation and decrypt

ARTICLE 19 is concerned that Section 21(3) problematically allows courts to compel individuals and entities to assist with investigations in ways that would contravene international standards on freedom of expression and privacy. Specifically, subsection (2)(d) allows for orders requiring any person with knowledge of a computer system to provide that information to a police officer to "enable" an investigation. Subsection (2)(e) allows for orders requiring any person with decryption information to grant access to such decryption

information. Subsection (2)(f) allows for orders requiring any individual with "appropriate technical knowledge" to provide that technical knowledge for purposes of executing a warrant.

The provision does not provide any definition or limitation for what "enable" entails. The vagueness of "enable" is especially problematic because it could mean anything from the forced disclosure of records, to commandeering service providers to become extensions of law enforcement. That might entail forcing providers to re-write computer code to insert security 'back doors' into their products or engage in active surveillance of users. ARTICLE 19 notes that encryption facilitates the exercise of free expression and privacy, and restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.

We note that in his 2015 report to the Human Rights Council, of the Special Rapporteur on Freedom of Expression[5] stipulated, in the case of orders for compelled assistance to decrypt communications, that such orders should be necessary and the least intrusive means available, based on publicly accessible law, clearly limited in scope focused on a specific target, and implemented under independent and impartial judicial authority. In the 2016 case of the US Federal Bureau of Investigation attempting to force Apple Computer to compel decryption of an iPhone device, the Special Rapporteur made a written submission to the judge reiterating the position that compelled assistance to decrypt communications raises grave concerns for freedom of expression.[6]

Recommendations:

- Subsections 21(3)(d) through 21(3)(f) allowing for investigative orders compelling technical assistance and decryption should be amended to specify that such orders can only be obtained when they are necessary, the least intrusive means available, and focused on a specific target.

[5] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye A/HRC/29/32, 22 May 2015.
[6] David Kaye, Re: In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 ED No. CM 16 - 10 (SP), March 2, 2016, *available at* http://apple.co/2crQepD.

About ARTICLE 19

ARTICLE 19 advocates for the development of progressive standards on freedom of expression and freedom of information at the international and regional levels, and their implementation in domestic legal systems. The Law Programme has produced a number of standard-setting publications which outline international and comparative law and best practice in areas such as defamation law, access to information and broadcast regulation.

On the basis of these publications and ARTICLE 19's overall legal expertise, the organisation publishes a number of legal analyses each year, comments on legislative proposals as well as existing laws that affect the right to freedom of expression. This analytical work, carried out since 1998 as a means of supporting positive law reform efforts worldwide, frequently leads to substantial improvements in proposed or existing domestic legislation. All of our analyses are available at http://www.article19.org/resources.php/legal.

If you would like to discuss this analysis further, or if you have a matter you would like to bring to the attention of the ARTICLE 19 Law Programme, you can contact us by e-mail at legal@article19.org. For more information about the ARTICLE 19's work in Kenya, please contact Henry Maina, Director of ARTICLE 19 Kenya, at henry@article19.org.