ARTICLE 19

Kenya: Cyber Security and Protection Bill

September 2016

Legal analysis

Executive summary

In September 2016, ARTICLE 19 reviewed the draft Cyber Security and Protection Bill (Draft Bill), which is currently being discussed in Kenya, for its compliance with international and regional human rights standards.

Our analysis shows that the Draft Bill is extremely problematic in this respect. In particular, it creates several broadly defined speech offences with harsh sentences that could have a dramatic chilling effect on freedom of expression online in Kenya. The provisions dealing with pornography, intimate images, and cyber-bullying fall well below permissible forms of content regulation under international standards on freedom of expression.

We recommend entirely omitting several offences that are either duplicative, or broadly defined as to expose them to abuse for less legitimate ends. These offences include, among others, cyber-squatting, which on their face conceivably punish many forms of legitimate expression. Eliminating these offences would simplify the law while still allowing the punishment of legitimately criminal conduct with greater legal certainty. We also recommend including more precise intent and harm requirements for existing offences, namely by requiring "dishonest" intent and "serious" harm to result for most sanctions.

Finally, 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.

The analysis not only highlights concerns and conflicts with international and regional human rights standards within the Draft Bill but also actively seeks to offer constructive recommendations on how the Bill can be improved.

Summary of recommendations:

- A clause should be inserted requiring that the Bill be interpreted in accordance with human rights standards, in particular the rights to privacy and freedom of expression and specifically reference international human rights standards;
- The number of offences should be greatly reduced. Offences related to content, that are not categories of content permissibly restricted under international human rights law, should be removed. Specifically, offences criminalising pornography should be removed;
- Offences 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;
- Penalties for most offences should be reduced from five years imprisonment or more to one or two years maximum;
- The Bill should provide more definitions for operative terms, including "access", "damage", "data", "intercept", "modification", and "traffic data;"
- The definition of "intimate image" should be stricken entirely. If a version is kept it should be amended to say "non-consensual intimate image" and require the image to be taken without the consent of the subject;
- "Cyber-security threat" should be amended to require "seriously adversely impact;"

- The definition of "computer" should closely follow the definition contained in Article 1 of the Cybercrime Convention and make explicit reference to "automatic processing of data"; and
- Section 9(2)(a) of the Draft Bill should be amended to require "preventing serious harm" as a prerequisite for information sharing agreements between private and public entities;
- Section 12(1) should be amended to include a definition of "unauthorised access" that at a minimum includes infringement of security measures without right;
- Section 12(1) should contain a heightened intentionality requirement of either "dishonest intent to gain access", or "intent to obtain computer data;"
- Section 13 should be amended to insert "serious" before "hindering", "interference", and "prevents;"
- The penalty carried by Section 14(1) should be reduced, for instance to a maximum of two years imprisonment; and
- Section 19 should be amended to remove "indirectly modifies or causes modification of" and replace it with "seriously hinders without right;"
- The penalties under Sections 17 and 18(1) should be reduced;
- Several provisions of the Draft Bill should be removed in their entirety, in particular Sections 12(2), 12(3), 31, 14(2), 14(3), 15, 16, 18(2), 18(3), 18(4), 20, 21, 22, 24, 27;
- Section 26 should, if it criminalises any form of child exploitation, define and criminalise the dissemination of child sexual abuse images ("child pornography") in accordance with accepted definitions such as that of the CoE Cybercrime Convention. Child exploitation without a computer can and should already be addressed by existing Kenyan criminal law;
- "Unlawfully" should be replaced with "intentionally" in Section 30; and
- Section 30 should provide a defence for producing or selling software for the purpose of training, testing, or protection of computer systems.

Table of contents

Introduction **5**

International human rights standards **6**

The protection of freedom of expression under international law 6

Prohibiting incitement to discrimination, hostility or violence 7

Terrorism and incitement to acts of terrorism 7

Online content regulation 8

Surveillance of communications 9

Anonymity and encryption 10

Cyber-crime 11

Analysis of the Draft Bill **13**

General comments 13

Definitions 14

Unlawful access to a computer system 15

Unlawful interceptions, misdirection, and interference 16

Forgery, fraud, and similar offences 17

Cyber-terrorism 18

Duty to report offences 18

Child sexual abuse images and child exploitation 19

Cyber-bullying 19

Content-based restrictions 20

Illegal devices and access codes 20

About ARTICLE 19 ..... **22**

Introduction

In this legal analysis, ARTICLE 19 reviews the 2016 Cyber Security and Protection Bill (the Draft Bill), [1] dated 5 July 2016, for its compliance with international human rights standards. In July 2014, ARTICLE 19 analysed the first draft of the Cybercrime and Computer related Crimes Bill (Cyber-crimes Bill) and in September 2016, the second version of the Cyber-crimes Bill. However, the Draft Bill, subject of this review, is a new bill introduced in the Senate which seems to address many of the same topics as the Cyber-crimes Bill.

Cyber security is currently a central issue in Kenya. The *Kenya Star* reported in September 2016 that businesses are very concerned about cybercrimes in light of rapid digitisation.[2] However, ARTICLE 19 believes that it is vital that Kenya's efforts to address these issues are consistent with its obligations to protect and promote freedom of expression under international law.

ARTICLE 19's analysis first sets out in detail such applicable international and regional human rights standards, in particular the right to freedom of expression and the right to privacy, together with guidance on how these provisions are interpreted in relation to information and communication technologies. It then goes on to make a number of general recommendations regarding the Draft Bill as a whole before highlighting human rights issues with particular sections of the Bill.[3]

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 urges the drafters of the Bill and the relevant committees in charge of scrutinising it to address the shortcomings identified in this analysis to ensure the compatibility of the Bill with international standards of freedom of expression. We stand ready to provide further assistance in this process.

[1] The Cyber Security and Protection Bill, 2016, p. 133, Kenya Gazette Supplement No. 110 (Senate Bills No. 12).
[2] Atul Shah, *Businesses can no longer ignore cyber security*, Kenya Star, 9 September 2016.
[3] 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.

International human rights standards

The protection of freedom of expression under international law

The right to freedom of expression is protected by a number of international human rights instruments that bind states, including Kenya, in particular Article 19 of the **Universal Declaration of Human Rights (UDHR)**[4] and Article 19 of the **International Covenant on Civil and Political Rights** (ICCPR).[5]

Kenya also ratified the 1983 African Charter on Human and Peoples' Rights (ACHPR) which guarantees the right to freedom of expression in Article 9.[6] Additional guarantees to freedom of expression are provided in the 2002 Declaration of Principles on Freedom of Expression in Africa (African Declaration) in Article II as well as the African Declaration on Internet Rights and Freedoms in Article III.[7]

Additionally, **General Comment No 34**,[8] adopted by the UN Human Rights Committee (HR Committee) in September 2011, explicitly recognises that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and Internet-based modes of expression.[9] In other words, the protection of freedom of expression applies online in the same way as it applies offline. State parties to the ICCPR are also required to consider the extent to which developments in information technology, such as Internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.[10] The legal framework regulating the mass media should take into account the differences between the print and broadcast media and the Internet, while also noting the ways in which media converge.[11]

Similarly, the four special mandates for the protection of freedom of expression, including the African Special Rapporteur on Freedom of Expression and Access to Information, have highlighted in their **Joint Declaration on Freedom of Expression and the Internet** of June 2011 that regulatory approaches in the telecommunications and broadcasting sectors cannot simply be transferred to the Internet.[12] In particular, they recommend the development of tailored approaches for responding to illegal content online, while pointing out that specific restrictions for material disseminated over the Internet are unnecessary. They also promote the use of self-regulation as an effective tool in redressing harmful speech.

As a state party to the ICCPR, Kenya must ensure that any of its laws attempting to regulate electronic and Internet-based modes of expression comply with Article 19 of the ICCPR as interpreted by the HR Committee and that they are in line with the special mandates' recommendations.

Limitations on the right to freedom of expression

[4] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[5] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[6] Kenya ratified the African Charter on Human and Peoples' Rights on 23 January 1992.
[7] Adopted at the 32nd Session of the African Commission on Human and Peoples' Rights, 17-23 October 2002; full text available at africaninternetrights.org.
[8] CCPR/C/GC/3, adopted on 12 September 2011, available at http://bit.ly/1xmySgV.
[9] *Ibid*, para. 12.
[10] *Ibid*, para. 17.
[11] *Ibid*, para. 39.
[12] Joint Declaration on Freedom of Expression and the Internet, June 2011, available at http://bit.ly/1CUwVap.

While the right to freedom of expression is a fundamental right, it is not guaranteed in absolute terms. Restrictions on the right to freedom of expression must be strictly and narrowly tailored and may not put in jeopardy the right itself. The determination whether a restriction is narrowly tailored is often articulated as a three-part test. Restrictions must:

- **Be prescribed by law**: this means that a norm must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.[13] Ambiguous, vague or overly broad restrictions on freedom of expression are therefore impermissible;
- **Pursue a legitimate aim:** exhaustively enumerated in Article 19(3)(a) and (b) of the ICCPR as respect of the rights or reputations of others, protection of national security, public order, public health or morals. As such, it would be impermissible to prohibit expression or information solely on the basis that they cast a critical view of the government or the political social system espoused by the government;
- **Be necessary and proportionate**. Necessity requires that there must be a pressing social need for the restriction. The party invoking the restriction must show a direct and immediate connection between the expression and the protected interest. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function. It must be shown that the restriction is specific and individual to attaining that protective outcome and is no more intrusive than other instruments capable of achieving the same limited result.[14]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[15]

Prohibiting incitement to discrimination, hostility or violence

It is also important to note that Article 20(2) ICCPR provides that any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence must be prohibited by law. At the same time, inciting violence is more than just expressing views that people disapprove of or find offensive.[16] It is speech that encourages or solicits other people to engage in violence through vehemently discriminatory rhetoric. At the international level, the UN has developed the Rabat Plan of Action, an inter-regional multi-stakeholder process involving UN human rights bodies, NGOs and academia - which provides the closest definition of what constitutes incitement law under Article 20 (2) ICCPR.[17]

Terrorism and incitement to acts of terrorism

There is no universally agreed definition of terrorism under international law.[18] At the same time, UN human rights bodies have highlighted the tension between freedom of expression and counter-terrorism measures. In particular, General Comment No. 34 clearly provides:

[13] HR Committee, *L.J.M de Groot v. The Netherlands,* No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).
[14] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[15] General Comment 34, *op.cit.*, para. 43.
[16] *C.f.* European Court, *Handyside v the UK*, judgment of 6 July 1976, para. 56.
[17] See UN Rabat Plan of Action (2012), available at http://bit.ly/1T2efOV. In particular, the Rabat Plan clarifies that regard should be had to six factors in assessing whether speech should be criminalised by states as incitement. These include the general context, the speaker, intent, content of the message or its form, the extent of the speech at issue and the likelihood of harm occurring, including its imminence.
[18] See e.g. UNODC, Frequently Asked Questions on International Law Aspects of Countering Terrorism, 2009, p. 4, available at http://bit.ly/1PQeTiC. See also UNODC, The Use of the Internet for Terrorist Purposes, 2012, para. 49, available at http://bit.ly/1X1yiTo.

> 46. States parties should ensure that counter-terrorism measures are compatible with paragraph 3. Such offences as "encouragement of terrorism" and "extremist activity" as well as offences of "praising", "glorifying", or "justifying" terrorism, should be clearly defined to ensure that they do not lead to unnecessary or disproportionate interference with freedom of expression. Excessive restrictions on access to information must also be avoided. The media plays a crucial role in informing the public about acts of terrorism and its capacity to operate should not be unduly restricted. In this regard, journalists should not be penalized for carrying out their legitimate activities.

Moreover, the **Johannesburg Principles on National Security, Freedom of Expression and Access to Information**[19] (Johannesburg Principles), a set of international standards developed by ARTICLE 19 and international freedom of expression experts, are instructive on restrictions on freedom of expression that seek to protect national security. Principle 2 of the Johannesburg Principles states that restrictions sought to be justified on the ground of national security are illegitimate unless their genuine purpose and demonstrable effect is to protect the country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force. The restriction cannot be a pretext for protecting the government from embarrassment or exposure of wrongdoing, to conceal information about the functioning of its public institutions, or to entrench a particular ideology. Principle 15 states that a person may not be punished on national security grounds for disclosure of information if

- the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or
- the public interest in knowing the information outweighs the harm from disclosure.

Further, the **Tschwane Principles on National Security and the Right to Information**[20] also consider extensively the types of restrictions that can be imposed on access to information.

Online content regulation

The above principles have been endorsed and further explained by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Special Rapporteur on FOE) in two reports in 2011.[21]

In the September 2011 report, the Special Rapporteur also clarified the scope of legitimate restrictions on different types of expression online.[22] He also identified three different types of expression for the purposes of online regulation:

- expression that constitutes an offence under international law and can be prosecuted criminally;
- expression that is not criminally punishable but may justify a restriction and a civil suit; and
- expression that does not give rise to criminal or civil sanctions, but still raises concerns

[19] Adopted on 1 October 1995. These Principles have been endorsed by the UN Special Rapporteur on FOE and have been referred to by the United Nations Commission on Human Rights in each of their annual resolutions on freedom of expression since 1996.
[20] The Tschwane Principles, available at http://osf.to/1jag6nW.
[21] Report of the UN Special Rapporteur on Freedom of Expression, A17/27, 17 May 2011 (May 2011 Report of the FOE SR) and Report of the UN Special Rapporteur on Freedom of Expression, A/66/290, 10 August 2011 (August 2011 Report of the FOE SR).
[22] *Ibid*, para. 18.

> in terms of tolerance, civility and respect for others.[23]

In particular, the Special Rapporteur on FOE clarified that the only exceptional types of expression that States are required to prohibit under international law are:

- "child pornography";
- direct and public incitement to commit genocide;
- hate speech; and
- incitement to terrorism.

He further made clear that even legislation criminalizing these types of expression must be sufficiently precise, and there must be adequate and effective safeguards against abuse or misuse, including oversight and review by an independent and impartial tribunal or regulatory body.[24] In other words, these laws must also comply with the three-part test outlined above. For example, legislation prohibiting the dissemination of child pornography over the Internet through the use of blocking and filtering technologies is not immune from those requirements.

Surveillance of communications

The right to privacy complements and reinforces the right to freedom of expression. The right to privacy is essential for ensuring that individuals are able to freely express themselves, including anonymously,[25] should they so choose. The mass-surveillance of online communications therefore poses significant concerns for both the right to privacy and the right to freedom of expression.

The right to private communications is strongly protected in international law through Article 17 of the ICCPR[26] that *inter alia*, states that no one shall be subjected to arbitrary or unlawful interference with his privacy, family or correspondence. In **General Comment No. 16** on the right to privacy,[27] the HR Committee clarified that the term "unlawful" means that no interference can take place except in cases envisaged by the law. Interference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives the ICCPR. It further stated that:

> [E]ven with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted. A decision to make use of such authorised interference must be made only by that authority designated under the law, and on a case-by-case basis.[28]

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that like restrictions on the right to freedom of expression under Article 19, restrictions of the right to privacy under Article 17 of the ICCPR should be interpreted as subject to the three-part test:

---

[23] *Ibid.*
[24] *Ibid*, para. 22.
[25] *Ibid*, para. 84.
[26] Article 17 states: 1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks".
[27] HR Committee, General Comment 16, 23rd session, 1988, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994).
[28] *Ibid.*, para 8.

> Article 17 of the Covenant should also be interpreted as containing the said elements of a permissible limitations test. Restrictions that are not prescribed by law are "unlawful" in the meaning of article 17, and restrictions that fall short of being necessary or do not serve a legitimate aim constitute "arbitrary" interference with the rights provided under article 17.[29]

In terms of surveillance (within the context of terrorism in this instance), he defined the parameters of the scope of legitimate restrictions on the right to privacy in the following terms:

> States may make use of targeted surveillance measures, provided that it is case-specific interference, on the basis of a warrant issued by a judge on the showing of probable cause or reasonable grounds. There must be some factual basis, related to the behaviour of an individual, which justifies the suspicion that he or she may be engaged in preparing a terrorist attack.[30]

The Special Rapporteur on FOE has also observed that:

> The right to privacy can be subject to restrictions or limitations under certain exceptional circumstances. This may include State surveillance measures for the purposes of the administration of criminal justice, prevention of crime or combatting terrorism. However, such interference is permissible only if the criteria for permissible limitations under international human rights law are met. Hence, there must be a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted under exceptional circumstances, and measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality.[31]

Anonymity and encryption

The protection of anonymity is a vital component in protecting the right to freedom of expression as well as other human rights, in particular the right to privacy. A fundamental feature enabling anonymity online is encryption - a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient" that protects the confidentiality of content against third-party access or manipulation.[32] Without the authentication techniques derived from encryption, secure online transactions and communication would be impossible.

The right to online anonymity has so far received limited recognition under international law. Traditionally, the protection of anonymity online has been linked to the protection of the right to privacy and personal data. In May 2015, the Special Rapporteur on FOE, published his report on encryption and anonymity in the digital age.[33] The report highlighted the following issues in particular:

---

[29] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, A/HRC/13/37, 28 December 2009, para 17.
[30] *Ibid*., para 21.
[31] May 2011 Report of the FOE SR, para. 59.
[32] SANS Institute, "History of encryption" (2001).
[33] 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.

- Encryption and anonymity must be strongly protected and promoted because they provide the privacy and security necessary for the meaningful exercise of the right to freedom of expression and opinion in the digital age;[34]

- Anonymous speech is necessary for human rights defenders, journalists, and protestors. He noted that any attempt to ban or intercept anonymous communications during protests was an unjustified restriction to the right to freedom of peaceful assembly under the UDHR and the ICCPR.[35] Legislation and regulations protecting human rights defenders and journalists should include provisions that enable access to and provide support for using technologies that would secure their communications;

- Restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law.[36] Laws and policies providing for restrictions to encryption or anonymity should be subject to public comment and only be adopted following a regular – rather than fast-track – legislative process. Strong procedural and judicial safeguards should be applied to guarantee the right to due process of any individual whose use of encryption or anonymity is subject to restriction.[37]

The Special Rapporteur's report also addressed compelled 'key disclosure' or 'decryption' orders whereby a government may "force corporations to cooperate with Governments, creating serious challenges that implicate individual users online".[38] The report stipulated that such orders should be

- based on publicly accessible law;
- clearly limited in scope focused on a specific target;
- implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets; and
- only adopted when necessary and when less intrusive means of investigation are not available.39

Cyber-crime

No international standard on cybercrime exists in the area.

In June 2014 Kenya became a party to the African Union Convention on Cyber-Security and Personal Data Protection (AU Cyber-Security Convention), not yet in force.[40] The AU Cyber-Security Convention stresses the importance of protecting fundamental rights including the right to freedom of expression. Article 25 requires states enacting cyber-security laws to ensure that such laws protect freedom of expression and adhere to regional conventions such as the African Charter on Human and Peoples' Rights. However, ARTICLE 19 finds that many articles of the AU Cyber-Security Convention do not comply with international freedom of expression standards, in particular the criminal penalties and content-based regulations present in the Convention fall short of the standards of permissible limitations on freedom of expression under other binding instruments to which Kenya is a party. The AU Cyber-Security

[34] *Ibid,* paras. 12,16 and 56.
[35] *Ibid,* para. 53.
[36] *Ibid,* para. 56.
[37] *Ibid,* paras. 31-35.
[38] *Ibid*, para. 45.
[39] *Ibid.*
[40] EX.CL/846(XXV), Malabo, 27 June 2014.

Convention does not require "dishonest" intent or "serious" harm for offences; nor does it provide for public interest defences for offences. Most problematically, it undertakes to criminalise several content-related offences. Some of these offences, including production or publication of child pornography, achieve legitimate ends that are consistent with permissible restrictions under Kenya's international human rights obligations. However, others, such as punishing insults based on political opinion, are overbroad and would proscribe expression that does not arise to illegitimate speech. The analysis will point out further discrepancies where appropriate.

From other regional standards, the 2001 Council of Europe Convention on Cybercrime (the CoE Cybercrime Convention) has been the most relevant standard.[41] Although Kenya is not a signatory to the Convention, it provides a helpful model for states seeking to develop cybercrime legislation in a way of comparative law. The CoE Cybercrime Convention provides definitions for relevant terms, including definitions for: computer data, computer systems, traffic data and service providers. It requires State parties to create offences against the confidentiality, integrity and availability of computer systems and computer data; computer-related offences including forgery and fraud; and content-related offences such as the criminalisation of child pornography. The CoE Cybercrime Convention then sets out a number of procedural requirements for the investigation and prosecution of cybercrimes, including preservation orders, production orders and the search and seizure of computer data. Finally, and importantly, it makes clear that the above measures must respect the conditions and safeguards for the protection of human rights and liberties, consistent with the ICCPR and other applicable international human rights instruments.

[41] 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.

Analysis of the Draft Bill

General comments

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

- **Failure to consider human rights framework and procedural safeguards:** Neither the "Memorandum of Objects and Reasons" nor the Draft Bill's preamble include any requirement that its provisions should be interpreted and implemented with due respect for human rights, in particular the rights to privacy and freedom of expression. We believe that the absence of any such provisions could threaten the entire Bill's compatibility with international standards and the enforcement of human rights in this area. While constitutional law purists might argue that this is not strictly speaking necessary because the Kenyan Constitution already protects the rights to freedom of expression and human rights in general, there would nevertheless be strong interpretative value in inserting a clause stating this given the impact of the Draft Bill on the enjoyment of human rights. This would help bring the Draft Bill in line with the international human rights law standards by stating that in case of doubt, the Draft Bill should be interpreted in line with human rights standards. This would also be consistent with best practice in this area, notably the CoE Convention on Cybercrime.

- **High number of offences:** The Draft Bill creates a very 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.[42] In our view, and as detailed further below, several or all of the offences provided for under the Draft Bill could be either regrouped, simplified, or entirely removed.

- **Content-related offences:** We also observe that the Draft Bill criminalises conduct based on content of communications or publications, particularly in the case of pornography, and attaches severe penalties of decades in prison. We note that pornography is not a category of content that can be blanketly restricted under international human rights law; for example, the Human Rights Committee has affirmed that restrictions on freedom of expression for the protection of public morals must be based on a broad understanding of what 'public morals' means.

- **Inclusion of "cyber terrorism" offence:** We are highly concerned about the breadth of "cyber terrorism" as an enumerated offence in Section 20 of the Draft Bill. The scope is particularly alarming because Section 20(1) allows for life imprisonment. The description "for purposes of terrorism" is vague and expands the scope of the Prevention of Terrorism Act, without requiring any serious harm to occur, but merely establishing intent to

[42] 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.

commit terrorism. The current reach of the Prevention of Terrorism Act has already been criticised by human rights organizations and the UN Special Rapporteur on Freedom of Peaceful Assembly and Association.[43] Further, the proposed offence does not differentiate between authorised and unauthorised use of a computer, only relying on "intent" to commit terrorism. The provision would therefore punish conduct that would not even be criminal under other offences of the Draft Bill, and could be used for illegitimate ends such as punishing an individual based on ideological political views or for acts of whistle-blowing.

- **Disproportionate sanctions and lack of public interest defence:** The offences contained in the Draft Bill are sanctions with unduly harsh sentences, including lengthy imprisonment of five years or more. We note that under international human rights framework, any restrictions on freedom of expression must be "proportionate."[44] 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.[45] In addition, a harm test or 'public interest defence' is not provided in the Draft Bill where appropriate.

Recommendations:

- A clause should be inserted requiring that the Bill be interpreted in accordance with human rights standards, in particular the rights to privacy and freedom of expression and specifically reference international human rights standards;
- The number of offences should be greatly reduced. Offences related to content, that are not categories of content permissibly restricted under international human rights law, should be removed. Specifically, offences criminalising pornography should be removed;
- Offences 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;
- Penalties for most offences should be reduced from five years imprisonment or more to one or two years maximum.

Definitions

ARTICLE 19 notes that this section contains relatively few definitions of key operative terms. In particular:

- Terms such as "access", "damage", "data", "intercept", "modification", and "traffic data" remain undefined;
- **T**he scope of the definition of "intimate image, is very concerning, particularly because there is no requirement that the image be taken or produced without the consent of the subject. As written it would appear to make production of consensual intimate photos a criminal act;

[43] Maina Kiai, On terrorism, the Executive wants to be the judge, jury and executioner, Daily Nation, 10 April 2015.
[44] *C.f.* also the AU Cyber-crime Convention, Article 31(1)(a).
[45] *C.f.* 1990 Act 3(6).

- The Draft Bill does not provide a definition of "damage" or clarify that only "serious" impairment or losses should attract criminal sanctions;
- Finally, although not included in the "Definitions" section, the defined guidelines for information sharing agreements in Section 9(2) are overbroad. Subsection 9(2)(a) particularly allows private entities to enter into information-sharing agreements simply to "ensure cybersecurity".

At the same time, we observes favorably that the Draft Bill requires serious harm for some terms, such as the inclusion of "debilitating impact" in the definition of "critical infrastructure." The definition of "computer" does not appear intrinsically problematic, although 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 CoE Cybercrime Convention.

Recommendations:

- The Draft Bill should provide more definitions for operative terms, including "access", "damage", "data", "intercept", "modification", and "traffic data;"
- The definition of "intimate image" should be stricken entirely. If a version is kept it should be amended to say "non-consensual intimate image" and require the image to be taken without the consent of the subject;
- "Cybersecurity threat" should be amended to require "seriously adversely impact;"
- The definition of "computer" should closely follow the definition contained in Article 1 of the Cybercrime Convention and make explicit reference to "automatic processing of data"; and
- Section 9(2)(a) of the Draft Bill should be amended to require "preventing serious harm" as a prerequisite for information sharing agreements between private and public entities.

Unlawful access to a computer system

Section 12 of the Draft Bill criminalises unauthorised access to a computer system, trafficking in passwords, and the use of anonymity devices. ARTICLE 19 is significantly concerned about the scope of these provisions and their compatibility with Kenya's obligations to protect and promote freedom of expression. Our key concerns relate to the following issues:

- *First,* Section 12(1) is unduly vague because it does not provide any definition for "without authorization." It is also overbroad because it does not require the infringement of security measures. Thus an individual that possesses access credentials to a computer system could nevertheless still be punished based purely on their intent upon accessing the system. The potential misuse of the provision is conceivable as Section 12(1) does not contain a sufficient intentionality requirement, such as "dishonest" intent or intent to obtain computer data as is recommended under Article 2 of the CoE Cybercrime Convention. As the provision is currently written, a whistleblower who possesses credentials to access a computer system and accesses materials for the purpose of informing the public of a matter of public concern could conceivably be violating the law.

- *Second,* the trafficking of passwords proscribed by Section 12(2) raises concerns because the phrase "without lawful authority" is nowhere defined. We note that while the AU Cyber-crime Convention undertakes to criminalise password sharing, the CoE Cybercrime Convention requires heightened intentionality, and such conduct is conceivably covered by other offences in the Bill such as unlawful access or fraud.

- *Third,* Section 12(3) broadly criminalises the use of anonymity devices with the intent to commit an offence. We believe this has a potential to chill the use of anonymity tools that are integral to exercising the right of expression.[46] For instance, some tools such as TOR are regularly used and promoted by human rights defenders and investigative journalists. The Special Rapporteur has articulated that restrictions on encryption and anonymity must meet the three-part test of limitations to the right to freedom of expression under international law. Section 12(3) is unnecessary to achieve a legitimate aim and therefore does not meet this standard.

- *Finally*, Section 31 is highly problematic because it forces employees to relinquish all codes and access rights "immediately upon termination of employment". The creation of criminal liability for failure to do so imposes an unreasonable burden on employees and the equivalent to a strict liability offence. The requirement also poses practical difficulties - i.e. an employee could be punished for inadvertently retaining access to their office e-mail system, an innocuous act in which many former employees engage. For this reason, Section 31 should be omitted entirely.

Recommendations:
- Section 12(1) should be amended to include a definition of "unauthorised access" that at a minimum includes infringement of security measures without right;
- Section 12(1) should contain a heightened intentionality requirement of either "dishonest intent to gain access", or "intent to obtain computer data;"
- Sections 12(2), 12(3) and 31 should be omitted entirely.

Unlawful interceptions, misdirection, and interference

Section 14 of the Draft Bill creates several offences, including interception of non-public transmissions by technical means, inducing a person in charge of electronic devices to deliver electronic messages, and intentionally hiding or detaining electronic mail, messages, or payments. Section 15 further criminalises the interception and destruction of electronic mail, and Section 16 punishes wilful misdirection of electronic messages.

ARTICLE 19 is concerned that these sections create an unnecessary number of duplicative offences. While Section 14(1) tracks the definition provided for in Article 3 of the CoE Cybercrime Convention, Sections 14(2) and 14(3) punish conduct that could already be dealt with under the prohibitions of forgery or fraud. There is no intentionality requirement provided for in Section 14(2) which punishes inducement of delivery of electronic messages. Sections 14(2), 15, and 16 all punish various forms of unlawful interferences with electronic messages which would seem to require their interception. Given the existing criminalisation of electronic message interceptions, ARTICLE 19 views that distinct offences are unnecessary.

Section 13 punishes the unauthorised interference with systems. The provision closely emulates the language of Article 5 of the CoE Cybercrime Convention except for the omission of any requirement that the hindering be "serious". Section 13 as written could thus

[46] *C.f.* the June 2015 report of the SR on FOE, *op.cit.*

proscribe trivial harm.

Section 19 similarly omits of any requirement that the modification be serious. As written the provision could criminalise trivial interferences. Section 19 should be amended to add "serious hindering without right" of a computer system.

Finally, the penalties under the provisions are unduly harsh, and ARTICLE 19 would suggest reduced sentences.

Recommendations:
- Section 13 should be amended to insert "serious" before "hindering", "interference", and "prevents;"
- Sections 14(2), 14(3), 15 and 16 should be removed entirely;
- The penalty carried by Section 14(1) should be reduced, for instance to a maximum of two years imprisonment; and
- Section 19 should be amended to remove "indirectly modifies or causes modification of" and replace it with "seriously hinders without right."

Forgery, fraud, and similar offences

ARTICLE 19 notes that the definition of "cyber forgery" provided for in Section 17 of the Draft Bill is consistent with that in the CoE Cybercrime Convention. The same is true of Section 18(1) punishing fraud. However, the following provisions are problematic from human rights perspective:

- Section 18 goes further that the provisions of the regional and comparative standards and also creates several problematic sub-offences. For instance, material misrepresentation, inscribing electronic messages, and manipulating computers with intent to shortpay all constitute conduct that could be dealt with as fraud under subsection 18(1), or under other provisions.

- The offences provided for in Sections 21 and 22, issuance of false e-instructions and phishing, are duplicative with forgery and fraud and are simply more specific versions of those offences. Similarly, identity theft and impersonation criminalised in Section 24 and cyber-squatting in Section 29 are duplicative. Sections 21, 22, 24, and 29 should therefore be deleted.

- Punishing "cyber-squatting" also raises significant freedom of expression concerns. It may inadvertently punish trivial and non-commercial acts of copyright infringement, preventing individuals from using copyrighted works in a way that is ordinarily protected by the defence of "fair use". Or it may be used to punish protest, parodies, or political commentary.

ARTICLE 19 finally observes that the punishments for forgery and fraud, five and three years imprisonment respectively, are unduly severe and should be reduced.

Recommendations:
- Sections 18(2), 18(3), and 18(4) should be deleted;
- The penalties under Sections 17 and 18(1) should be reduced; and

- Sections 21, 22, 24, and 29 are simply more specific versions of forgery and fraud and carry similar penalties - it is therefore duplicative to keep them and they should be deleted.

Cyber-terrorism

Section 20 of the Draft Bill punishes accessing a computer for the purposes of terrorism.

ARTICLE 19 objects the overreaching breadth of Section 20 and we questions the necessity of a separate cyber terrorism offences in this legislation. We also note that the existing scope of the Prevention of Terrorism Act from which Section 20 draws its definition has already been criticised by human rights organizations and experts.[47]

We are also concerned that Section 20(1) provides a severe penalty of life imprisonment for simply an access offence. There is no public interest defence. The provision also does not differentiate between 'authorised' access and 'unauthorised' access. Thus, Section 20 could more severly punish conduct that would not even constitute unauthorised access under Section 12.

To illustrate the problem, a whistleblower with authorised access to a government computer system, such as Edward Snowden, who accesses that computer system with the intent of disseminating material to journalists in the public interest. The whistleblower would not run afoul of Section 12 because he or she would be authorised to access the materials. However, it is possible that the individual could be prosecuted and face life imprisonment under Section 20, without any opportunity to make arguments in the public interest.

For these reasons the cyber terrorism offence falls far short of principles of legal certainty or proportionality under human rights law.

Recommendations:

- Due to lack of precision, potential for abuse, highly severe penalty of life imprisonment, and the sufficiency of other instruments that do not contain terrorism offences, Section 20 should be struck out in its entirety.

Duty to report offences

Section 23 requires individuals and entities to affirmatively report all cyber intrusions to the government and carries criminal penalties for failure to do so—regardless of any of the enormous practical difficulties such a system presents. Section 23(1) requires any person operating a computer system or network to "immediately inform" and submit a report to the National Cyber Threat Response Unit of any "attacks, intrusions and other disruptions". The report must be submitted within seven days.

ARTICLE 19 finds that this reporting requirement is highly problematic for several reasons.

- *First*, criminal law generally does not impose on bystanders an affirmative duty to report crimes, for the reason that it would often amount to a strict liability offence without any

[47] Maina Kiai, On terrorism, the Executive wants to be the judge, jury and executioner, Daily Nation, 10 April 2015.

requisite *mens rea* or criminal intent. But Section 23 imposes such a strict liability offence.

- *Second*, imposing a reporting requirement in the computer crimes context presents incredible practical difficulties. Attribution is a well-known issue for computer crimes as it can often be impossible to ascertain whether an error in a computer or system is caused by an attack or simply a bug. Generally speaking, it is usually more advantageous for attackers in a system to exploit bugs without making their presence known. It can often be unclear whether an error is computer- or human-caused. System administrators deal with bugs and errors on a regular basis; larger systems may have them occur frequently. Having to report every single error for fear that it may actually be an attack—because criminal liability attaches—would create near-impossible tasks for many administrators.

We note that the 2015 report of the Special Rapporteur on FOE 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.

Recommendation:

- Section 23 should be omitted in its entirety because it presents enormous practical difficulties in complying with reporting requirements that carry criminal penalties. Requirements for compelled assistance must be necessary and the least intrusive means available and clearly limited in scope.

Child sexual abuse images and child exploitation

We note that criminalising "child pornography" (child sexual abuse images) online is a legitimate restriction and is consistent with the recommendations of the UN Special Rapporteur on freedom of expression and the CoE Cybercrime Convention. We however observe that Draft Bill as written does not criminalise child pornography (a legitimate aim), while attaching severe penalties in Section 25 to normal pornography (an illegitimate aim).

Further, the offence articulated in Section 26 does not necessarily center on computer-related conduct, instead criminalising the solicitation of children. This activity can be proscribed by the regular criminal law. To the extent that Kenyan law fails to provide sufficient protection for child exploitation, the legislature should take immediate steps to ensure that the criminal law is adequate and fit for the purpose.

Recommendation:

- Section 26 should, if it criminalises any form of child exploitation, define and criminalise the dissemination of child sexual abuse images ("child pornography"). Child exploitation without a computer can and should already be addressed by existing Kenyan criminal law.

Cyber-bullying

ARTICLE 19 expresses concern that Section 27, criminalizing cyber-bullying, is extremely

vague and ultimately fails to comply with requirements on legitimate restrictions on expression under international human rights law.

It is legitimate for the state to 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. However, the Draft Bill is an inappropriate venue for addressing the issue. It is unclear why normal statutes on assault or threats are inappropriate to apply in the digital context.

The penalty of up to five years is also harsh, and no public interest defence is provided.

Recommendation:

- Section 27 should be struck in its entirety. Measures stalking and harassment should be addressed by the general criminal law, rather than by cybercrime legislation. Further, such legislation would at a minimum need to make available a public interest defence.

Content-based restrictions

Sections 25 and 28 criminalise with severe penalties the transfer and publication of certain types of pornographic materials, including intimate images.

ARTICLE 19 is very concerned that these provisions are unduly broad, restrictive, and open to subjective interpretation and abuse. We reiterate that pornography is not a form of expression that may be restricted under international law. The HR Committee has affirmed that restrictions on freedom of expression for the protection of public morals must be based on a broad understanding of what 'public morals' means.

Section 28 provides no intent requirement at all while proscribing publication.

The penalties for these provisions are among the highest in the statute aside from terrorism. At thirty and twenty years imprisonment, respectively, they are incredibly disproportionate punishments for conduct that is not even an offence in relevant international instruments.

Recommendation:

- Sections 25 and 28 should be struck out entirely.

Illegal devices and access codes

Section 30 of the Draft Bill criminalises anyone who “unlawfully” manufactures, adapts, sells, procures, imports or distributes devices or programs adapted primarily for the purpose of committing an offence under the Bill.

ARTICLE 19 notes with concern that Section 30 is overbroad because “unlawfully” is nowhere defined. There is no intentionality requirement, which would seem to criminalise dual-purpose software. Many companies would know that software they produce could be used for multiple purposes, including unauthorised access to systems. Intentionality is the same standard required under Article 6 of the CoE Cybercrime Convention, and should thus be inserted.

We are also concerned that 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, there is no defence for the training, testing, or protection of computer systems. As a result legitimate security research and testing could be criminalised by Section 30 of the Bill.

Recommendations:

- "Unlawfully" should be replaced with "intentionally" in Section 30; and
- Section 30 should provide a defence for producing or selling software for the purpose of training, testing, or protection of computer systems.

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.