Kenya: Computer and Cybercrimes Bill 2017

April 2018

Legal analysis

Executive summary

In April 2018, ARTICLE 19 reviewed the draft Computer and Cybercrimes Bill, 2017 (Draft Cyber-crimes Bill) of Kenya, currently submitted to the National Assembly for approval. This is the third contribution of ARTICLE 19 to the drafting process.

Our analysis shows that the Draft Cybercrimes Bill contains several important additions that are apparently modelled after relevant international standards. 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.

ARTICLE 19 urges drafters of the Bill to address its inconsistencies with human rights standards before it is voted on in the National Assembly. We also urge the National Assembly to incorporate these comments into the final version of the Bill.

Summary of key recommendations:

- The definition of "computer system" should explicitly limit its scope to systems that engage in automatic processing of data. The definition of "content data" should remove references to the "meaning or purport" of the communication. The definition of "damage" should be added and require serious impairment or loss to a computer system or to specified legitimate national security or public order interests;
- Section 4(1) should only penalize unauthorized access as described in the provision if it is committed with intent to obtain computer data or other "dishonest" intent. The Bill and/or implementing regulations should also provide examples of "dishonest" intent;
- The following sections should be removed in their entirety: Section 4(3), Section 5(2), Section 8(2), Section 9, Section 10, Section 10(2), Section 11, Section 12, Section 14(2), Section 16, and Section 17;
- Section 5(1) should require "intent to commit specific and serious offences" and specify all the offences that would trigger liability under this Section;
- Section 7(1) of the Draft Bill should be amended to require serious damage or impairment;
- Section 8(1) should replace "knowingly" with "intentionally;"
- Section 10(2) should also limit the definition of a "protected computer system" to those systems that are necessary for a specified range of legitimate national security and public safety purposes;
- The Bill should establish a public interest defence against offences specified in Part II for "any person who discloses information that he or she reasonably believes, at the time of disclosure, to be true and to constitute a threat or harm to a specified public interest, such as a violation of national or international law, abuse of authority, waste, fraud or harm to the environment, public health or public safety;"
- Sections 14 and 15 should be drafted consistently with existing criminal laws on fraud and forgery to avoid duplication or contradiction;
- Section 14(1) should incorporate the requirement of dishonest intent;
- Any attempt to regulate cyber stalking or cyber bullying should be developed in consultation with a meaningful and representative cross-section of civil society, academics, the technology and media industry and other relevant non-State actors;

- Section 18 should expressly state that internet service providers are exempt from liability with respect to any offence committed by a third party under the Bill when they are acting as mere conduits, or merely performing hosting, caching or information location functions;
- Section 18 should clarify that the Bill does not impose general obligations on internet service providers to monitor the information which they transmit or store, or to actively seek facts or circumstances indicating illegal activity;
- Sections 23(3)(d) through 23(3)(f) should permit warrants compelling decryption, technical assistance and government access to communications and communications data only when such orders are necessary and the least intrusive means available to conduct a specific and legitimate investigation, and focused on a specific target.

Table of contents

Introduction 5
International human rights standards 6
Analysis of the Draft Bill 9
Definitions 9
Offences 9
Content related offences 15
False Publications 15
"Child pornography" 15
Cyberstalking and cyber-bullying 16
Corporate liability 16
Investigative procedures and legal assistance 17
Search and Seizure of Stored Computer Data 17
About ARTICLE 19 19

Introduction

In April 2018, ARTICLE 19 analysed the Draft Computer and Cybercrimes Bill, 2017 (the Draft Bill) of Kenya[1] for its compatibility with international human rights standards. The Draft Bill is currently pending an approval in the Kenyan National Assembly.

This analysis is our third contribution to the drafting process of this Bill as we analysed the first draft of the Bill in July 2014,[2] and a subsequent version in September 2016.[3] Additionally, ARTICLE 19 has also previously analysed related legislative and policy proposals, including the Draft Guidelines on dissemination via Electronic Communications Networks[4] in July 2017, and the Cyber Security and Protection Bill in July 2016.[5] This analysis should be read in conjunction with the previous comments to earlier versions of the Draft Bill.

Our analysis is based on Kenya's obligations under international standards on freedom of expression and related human rights, particularly as they apply to digital media and the domestic guarantees to freedom of expression in the Kenyan Constitution. This analysis not only examines human rights concerns with specific sections of the Bill, but also offers concrete recommendations on how each section discussed below may be modified to ensure their compatibility with international standards. While ARTICLE 19 focuses on freedom of expression concerns with the Bill, the fact that there are no comments on particular sections does not signal our endorsement.

ARTICLE 19 urges drafters of the Bill to address its inconsistencies with human rights standards before it is voted on in the National Assembly. We also urge the National Assembly to incorporate these comments into the final version of the Bill.

We stand ready to provide further assistance in bringing the Bill in full compliance with Kenya's human rights obligations.

[1] The text of the Draft Bill is available at https://bit.ly/2C0QkfH.
[2] ARTICLE 19, Cybercrime and Computer Related Crimes Bill, 2014, available at https://bit.ly/1H0PICH.
[3] ARTICLE 19, Kenya: Computer and Cybercrimes Bill, September 2016, available at https://bit.ly/2v1YrKM.
[4] ARTICLE 19, Kenya: New Draft Guidelines on dissemination via Electronic Communications Networks should be scrapped, 28 July 2017, available at https://bit.ly/2GOdNI4.
[5] ARTICLE 19, Kenya: Cyber Security and Protection Bill, September 2016, available at https://bit.ly/2v1YrKM.

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),[6] Article 19 of the International Covenant on Civil and Political Rights (ICCPR),[7] Article 9 of the **African Charter on Human and Peoples' Rights** (ACHPR)[8] and in other regional standards developed in the region.[9]

Importantly, the General Comment No 34,[10] adopted by the UN Human Rights Committee (HR Committee), explicitly recognises protection of the right to freedom of expression in relation to all forms of electronic and Internet-based modes of expression.[11] 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.[12]

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 2011 Joint Declaration on Freedom of Expression and the Internet recommended 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. [13]

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

Under human rights standards, the right to freedom of expressions can be limited under certain circumstances - often articulated as a three-part test. Restrictions must:

- Be prescribed by law: this means that a norm must be formulated with sufficient precision;[14] ambiguous, vague or overly broad restrictions are impermissible;

- Pursue a legitimate aim: exhaustively enumerated in Article 19(3)(a) and (b) of the

[6] UN General Assembly Resolution 217A(III), adopted 10 December 1948.
[7] GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.
[8] Kenya ratified the African Charter on Human and Peoples' Rights on 23 January 1992.
[9] See, in particular 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.
[10] CCPR/C/GC/3, adopted on 12 September 2011, available at http://bit.ly/1xmySgV.
[11] *Ibid*, para. 12.
[12] *Ibid*, para. 17.
[13] Joint Declaration on Freedom of Expression and the Internet, June 2011, available at http://bit.ly/1CUwVap.
[14] HR Committee, *L.J.M de Groot v. The Netherlands,* No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).

ICCPR as respect of the rights or reputations of others, protection of national security, public order, public health or morals;

- Be necessary and proportionate. Necessity requires that there must be a pressing social need for the restriction. Proportionality requires that a restriction on expression is not over-broad and that it is appropriate to achieve its protective function.[15]

The same principles apply to electronic forms of communication or expression disseminated over the Internet.[16]

Additionally, Article 20(2) of the ICCPR obliges States to prohibit by law "any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence." In General Comment No. 34, the HR Committee stressed that while States are *required* to prohibit such expression, these limitations must nevertheless meet the strict conditions set out in Article 19(3).[17]

Kenya must adhere to these principles in the domestic legislation, including in relations to the issues addressed in the Draft Bill.

Cybercrime

No international standard on cybercrime exists in the area. The 2014 African Union Convention on Cyber Security and Personal Data Protection (African Union Convention) [18]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's view is that 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 analysis will point out such discrepancies where appropriate.

Namely, the African Union Convention does not require "dishonest" intent or "serious" harm for offences; nor does it provide for public interest defences for offences. Most problematically, the African Union Convention 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.

From the regional standards, the 2001 Council of Europe Convention on Cybercrime (the Cybercrime Convention) has been the most relevant standard.[19] Although Kenya is not a signatory to the Convention, it provides a helpful model for states seeking to develop cybercrime legislation.

[15] HR Committee, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
[16] General Comment 34, *op.cit.*, para. 43.
[17] HR Committee, General Comment No. 34, 21 June 2011, CCPR/C/GC/34, para. 52.
[18] The 2014 African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014.
[19] 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.

The 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 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, the Cybercrime Convention 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.

Analysis of the Draft Bill

Definitions

Part I of the Bill establishes several important definitions, including "access," "computer data storage medium," "computer system", "data," "content data", "interception," "interference," "subscriber information," and "traffic data."

ARTICLE 19 welcome the fact that the definitions of "data," "service provider," and "traffic data" are consistent with the definition contained in the Council of Europe Cybercrime Convention (CoE Cybercrime Convention) which is an important comparative standard.[20] However, several key definitions could be improved, including the following:

- *Computer system*: This definition does not include a reference to "automatic processing of data," a key component of the definition of "computer system" (as for instance outlined in the CoE Cybercrime Convention);

- *Content data*: The definition of "content data" includes not only the substance of a specified communication, but also "its meaning or purport." ARTICLE 19 is concerned that this is too broad, and may lead to the surveillance and restriction of communications that do not have a sufficient link to a specific investigation or offence;

- *Damage*: The Draft Bill does not contain a definition of "damage." It should clarify that only serious harm, impairment or loss to a computer system or specified legitimate national security and public order interests should attract criminal sanctions.

Recommendations

- The definition of "computer system" should explicitly limit its scope to systems that engage in automatic processing of data;
- The definition of "content data" should remove references to the "meaning or purport" of the communication;
- The Bill should establish a definition of "damage" requiring serious impairment or loss to a computer system or to specified legitimate national security or public order interests.

Offences

Part II of the Draft Bill establishes two main categories of offences: nine offences relating to the mishandling of computer systems or data (Sections 4, 5, 6, 7, 8, 9, 11, 14, and 15) and three relating to content (Sections 12, 13 and 16). Part II also establishes enhanced penalties for certain offences (Section 10), liability for aiding and abetting the commission of offences (Section 17), and corporate liability for offences (Section 18).

Before addressing specific issues with the Draft Bill, ARTICLE 19 wishes to express the following general concerns:

- Unusually high number of offences, including overlapping offences: As we observed in the earlier analysis of the Draft Bill, it introduces an unusually high number of computer-

[20] Note that the definition of "data" under the Bill is the same as the definition of "computer data" under the CoE Cybercrime Convention.

related offences. In comparison, the CoE Cybercrime Convention contains only five such offences, and the UK Computer Misuse Act 1990 contains only four such offences. To our knowledge, neither States parties to the Convention nor the UK has raised concern that these offences are insufficient to deal with cybercrime. Moreover, the Bill contains separate offences for unauthorized access and interception, and separate offences for computer forgery or fraud. The substantial overlap between these offences creates concern that individuals will be charged under separate offences for the same crime, enhancing the risk of excessive criminal liability;

- Content-related offences are unnecessary and disproportionate: Offences criminalizing the exchange of particular types of content, including false publications and communications that "detrimentally affects a person," are likely to violate Kenya's obligations to respect and ensure freedom of expression. These offences are excessively broad and provide the authorities largely unfettered discretion to prosecute individuals for expression and communication that is perfectly legitimate and lawful. Their potential impact and chilling effect on minorities, civil society, academics and political opposition is particularly concerning. We recommend removing most of these offences;

- Disproportionate sanctions: We are concerned that the offences provide for unduly harsh penalties, including lengthy custodial sentences. Moreover, most of the offences do not require the dishonest intent or serious harm in connection with the offence before criminal sanctions attach. We therefore recommend that offences against the confidentiality, integrity and availability of computer data and systems should be reduced to a maximum of twelve months. A general public interest defence should also be introduced and properly defined.

Offences related to the mishandling of computer systems or data

Unauthorized access

Section 4 of the Draft Bill punishes anyone who infringes the security measures of a computer system with "intent to gain access" to that system and knowledge that such access is unauthorized.

ARTICLE 19 reiterates the *mens rea* for this offense falls short of international standards. Since mere intent to gain access would trigger liability, the testing of computer systems for security purposes could inadvertently become criminalized. Section 4 should specify that unauthorized access is only punishable if it is committed to obtain computer data or other "dishonest" intent.

Recommendations

- Section 4(1) should only penalize unauthorized access as described in the provision if it is committed with intent to obtain computer data or other "dishonest" intent. The Bill and/or implementing regulations should also provide examples of "dishonest" intent;
- Section 4(3), which states that the offense does not require unauthorized access to be directed at any program or data, should be removed its entirety.

Access with Intent to Commit Further Offence

Section 5 makes it an offence for anyone who violates Section 4 with "intent to commit a further offence under any law" or facilitate its commission. This offence is punishable with a fine of up to 10 million shillings, ten years' imprisonment or both.

ARTICLE 19 has previously raised concern that the *mens rea* for this offence fails to comply with the requirement of legal certainty under international law, and should be limited to intent to commit both specific and serious offences. The risk of illegitimate prosecution under Section 5 is significantly heightened given the potentially broad scope of criminal liability for "false publications" under Section 12 and "cyber stalking and cyber-bullying" under Section 16.

The *actus reus* for this offence also appears to be overbroad, failing to clearly establish that Section 4 violations trigger liability under Section 5 only if they serve as a means or preparatory act to the commission of a further offence.

We again question the necessity of Section 5 given that the Bill already criminalizes unauthorized access (under Section 4) and knowingly or willfully aiding or abetting any offence under (Section 17). Furthermore, the aiding or abetting of serious offences, whether through unauthorized access or any other means, would already be penalized under existing criminal laws.

Recommendations

- Section 5(1) should require "intent to commit specific and serious offences" and specify all the offences that would trigger liability under this Section;
- Section 5(2) should be removed in its entirety.

Unauthorized Interception

Section 7(1) of the Draft Bill makes it an offence to intentionally cause an "interception" with a computer system without authorization and in a manner that causes the "transmission of data" to or from that system. Section 2 specifies that "interception" refers to the "monitoring, modifying, viewing or recording of non-public transmissions of data to or from a computer system". This offence is punishable with a fine of up to 10 million shillings and/or 5 years' imprisonment.

ARTICLE 19 notes with appreciation that the offence only applies to the transmission of non-public data. We also appreciate the clarification that Section 7 applies only to interception that meets specified conditions and not merely any interference with a computer system.

However, we are concerned that the offence is still overbroad and does not establish a sufficient harm requirement. For comparison, we note that Section 5 of the CoE Cybercrime Convention provides that system interference is punishable if it "seriously hinder[s] without right the functioning of a computer system." This implies a requirement that the interception should be a criminalized only if it creates serious damage or impairment.

Recommendation:

- Section 7(1) of the Draft Bill should be amended to require serious damage or impairment;

Illegal devices and access codes

Section 8(1) makes it an offence to "knowingly" manufacture, adapt, sell, procure, import, supply, distribute or otherwise make available devices or programs designed or adapted primarily for the purpose of committing an offence under the Bill. Section 8(2) specifically criminalizes anyone who knowingly receives or is in possession of such devices or programs without "sufficient excuse or justification."

While ARTICLE 19 appreciates the inclusion of the Section 8(3)(a) proviso that exempts the training, testing or protection of computer systems from liability, we are still concerned that the offence is overbroad and disproportionate:

- The requirement of knowledge (as opposed to intent) would unduly implicate the provision of dual-use technologies, which has both legitimate and illegitimate purposes. Such dual-use technologies could include encryption and anonymity tools (such as Virtual Private Networks ("VPNs"), proxy networks and anonymizing software), which may be implicated in illegal activity but could also be used to prevent criminal or undue State intrusion into private communications. Accordingly, Section 8(1) should establish the more stringent *mens rea* requirement of "intent;"

- Furthermore, Sections 8(1) and 8(2) could be broadly interpreted to prosecute individuals or companies that provide or use software and other tools to capture video or audio streams. While these tools could be used to facilitate copyright infringement, they also have significant non-infringing uses, such as downloading content licensed under a Creative Commons license or for purposes of "fair use." We also reiterate our concern that Section 8 could be used to penalize the dissemination of software used to break Digital Rights Management (DRM) systems, which have been criticized for restricting trivial and non-commercial acts of copyright infringement after sale (such as transferring data between the buyer's own digital devices), and non-infringing uses of copyrighted digital material (such as fair use).

Recommendations:

- Section 8(1) should replace "knowingly" with "intentionally;"
- Section 8(2) should be removed.

Unauthorized Disclosures of Passwords

We reiterate our concern with Section 9 of the Draft Bill, which criminalizes anyone who knowingly discloses a password or access code without authority. The requirement of "knowledge," which is a substantially lower threshold than intentionality, could criminalize a range of legitimate activities, including security testing and research or the sharing of passwords for academic and personal use.

Recommendation:

- Section 9 should be removed entirely.

Enhanced penalties

Section 10(1) of the Draft Bill provides enhanced penalties for violations of Sections 4, 5, 6 and 7 on a "protected computer system." Section 10(2) defines a protected system as one that is used for, among other purposes, "the security, defence or international relations of Kenya" or "the protection of public safety," and any system that the Cabinet Secretary "may

consider appropriate" to designate as such. Offences that satisfy this criteria are punishable with a fine of up to twenty five million shillings and/or twenty years' imprisonment.

ARTICLE 19 is concerned that the definition of a "protected computer system" is tied to vague and open-ended functions, such as protecting Kenya's "international relations" or "public safety." This lack of specificity, coupled with the Cabinet Secretary's unlimited authority to designate protected computer systems, would give the authorities excessive discretion to impose severe penalties, enhancing the risk of disproportionate sanctions.

Recommendations:

- Section 10 of the Draft Bill should be removed entirely;
- In the alternative, Section 10(1) should limit enhanced penalties to offences that cause serious damage or impairment to a "protected computer system;"
- Section 10(2) should also limit the definition of a "protected computer system" to those systems that are necessary for a specified range of legitimate national security and public safety purposes;
- Section 10(2)(f) should be removed;
- The enhanced penalties should be significantly reduced.

Cyber espionage

"Cyber espionage" is prohibited in Section 11 of the Draft Bill:

- Section 11(1) establishes the offence of "cyber espionage" for the unauthorized access to or interception of "critical" data, databases or "a national critical information infrastructure;"

- Section 11(2) renders a person liable for cyber espionage if s/he unlawfully possesses or transmits data to, from or within a "critical database" or a "national critical information infrastructure" with the intent to benefit a foreign state against Kenya;

- Section 11(3) makes it an offence to gain access or intercept data that is "in possession of the State" and exempt from Kenya's law on access to information with the intention to benefit a foreign state against Kenya.

Section 11(1) and 11(2) offences are punishable with up to twenty years' imprisonment and/or a fine of ten million shillings. Section 11(3) offences are punishable with a fine of up to five million shillings and/or ten years' imprisonment.

ARTICLE 19 is extremely concerned that these provisions are vaguely formulated, unnecessary and disproportionate. In particular:

- The draft Bill does not define which databases or infrastructure are considered "critical," providing the authorities with excessive leeway to prosecute unauthorized data access and interception offences as cyber espionage based on vague and unaccountable criteria;

- While we appreciate Section 11(3)'s reference to the 2016 Access to Information Act, we are concerned that this section will impose severe criminal penalties on information disclosures that are not authorized under the Act but nevertheless in the public interest;

- The intentionality requirement does not explain what constitutes a "benefit" to a foreign state, exacerbating concerns of vagueness and the threat of government overreach. Given

the gravity of espionage offences, the Bill should require intent to cause serious harm to specified legitimate national security interests;

- The penalties are unduly severe.

Recommendations:
- Section 11 of the Draft Bill should be removed entirely, and incidents of cyber espionage should be addressed under existing espionage laws (which should also fully comply with the international freedom of expression standards);
- In the alternative, all Section 11 offences should require intent to cause serious harm to specified legitimate national security interests. The definition of "critical" databases or infrastructure should be clarified;
- The penalties should be significantly reduced.

Lack of 'public interest' defences

ARTICLE 19 notes with concern that the Bill does not provide for 'public interest' defences, such as a defence for unauthorized disclosures of computer data that nevertheless expose fraud, waste or abuse. This defence would be consistent with the UN Special Rapporteur's recommendation under Article 19 of the ICCPR.[21] The lack of such defences heightens the risk that government and private whistle-blowers will be unfairly prosecuted, enhancing the chilling effect on critical public disclosures of wrongdoing and other information the public has a legitimate interest in knowing.

Recommendation:
- The Bill should establish a public interest defence against offences specified in Part II for "any person who discloses information that he or she reasonably believes, at the time of disclosure, to be true and to constitute a threat or harm to a specified public interest, such as a violation of national or international law, abuse of authority, waste, fraud or harm to the environment, public health or public safety."

Computer forgery and fraud

Section 14(1) of the Draft Bill makes it an offence to intentionally input, alter, delete or suppress computer data if it results in "inauthentic data" with the intent that it be acted upon for legal purposes. Section 15(1) criminalizes the gaining of economic benefit or causing a loss to another person via the unauthorized use of a computer system with dishonest intent.

Although ARTICLE 19 has noted in the past that both offences are largely consistent with the CoE Cybercrime Convention, we remain concerned that these sections would criminalize behavior using a computer that is already criminalized offline. We encourage the government to ensure these sections are drafted consistently with existing laws.

ARTICLE 19 is also concerned that Section 14(2) doubles the maximum penalties for "dishonest intent," while the CoE Cybercrime Convention suggests dishonest intent is a foundation for criminal liability.

We also reiterate our concern that Section 15(2) is unduly complex and should be simplified.

[21] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/70/361, 8 September 2015.

Recommendations

- Sections 14 and 15 should be drafted consistently with existing criminal laws on fraud and forgery to avoid duplication or contradiction;
- Section 14(1) should incorporate the requirement of dishonest intent;
- Section 14(2) should be removed entirely. At minimum, it should limit proscribed activities to "any input, alteration, deletion or suppression of computer data" and "any interference with the functioning of a computer system."

Content related offences

False Publications

Section 12 of the Draft Bill makes it an offence to "intentionally publis[h] false, misleading or fictitious data" or "misinfor[m] with intent that the data shall be considered or acted upon as authentic," with penalties of up to 15 million shillings, two years' imprisonment or both.

ARTICLE 19 is gravely concerned that this sweeping criminalization of "false publications" would effectively arrogate to authorities the role of determining "truth" in public discourse, severely curtailing independent journalism, civic engagement and other activities essential to a democratic society. The vague prohibition of "false" and "misleading" data, for example, is highly subjective and prone to abuse, providing authorities with a pretext to prosecute reporting, criticism or commentary they disagree with or find controversial. The prohibition on publication of "fictitious data" could also be broadly interpreted to penalize writers, bloggers, artists and anyone publishing satirical or comedic material online.

The prohibition against misinformation also penalizes the inadvertent publication of inaccurate information, holding online users to unrealistic standards of factual accuracy under the threat of grave criminal penalties. The intent requirement is redundant, since a person who inadvertently publishes inaccurate data would reasonably (albeit mistakenly) believe in its authenticity at the time of publication. This prohibition is likely to disproportionately chill journalists, civil society, and others engaged in reporting and analyzing rapidly unfolding news stories and other fast-paced developments.

Recommendation:

- Section 12 of the Draft Bill should be removed in its entirety. The authorities should explore less intrusive measures for addressing disinformation and propaganda, including providing subsidies or other forms of financial or technical support for media and news literacy programs and independent and human rights-compliant mechanisms for media self-regulation (such as press complaints bodies or ombudsmen).

"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.

Cyberstalking and cyber-bullying

Section 16 makes it an offence for a person to "willfully and repeatedly" communicate "directly or indirectly" with someone else if they "know or ought to know" that such conduct "is likely to cause those persons apprehension or fear of violence" or "detrimentally affects that person."

ARTICLE 19 reiterates its concerns from its analyses of previous versions of the Bill: these provisions raise serious inconsistencies with the requirements of legal certainty, necessity and proportionality under international human rights law.

We appreciate the government's need to protect individuals from harassment, threats and other forms of intimidation. However, "apprehension or fear of violence" establishes an exceedingly low threshold for criminality, threatening to penalize anyone who publishes or reposts content that raises the possibility of violence. In particular, we are concerned that this provision could be triggered to target reporting and commentary on incidents or patterns of violence connected to government or powerful private actors, such as civil conflict or the violent suppression of legitimate protests.

The prohibition on communication that "detrimentally affects" a person is even broader, potentially penalizing any form of expression that, if sufficiently repeated or disseminated, has a perceived negative impact on someone else.

While ARTICLE 19 acknowledges that Section 16(3)(c) establishes a public interest defence in "particular circumstances," the failure to define or explain what constitutes the "public interest" makes it impossible for defendants and the broader public to reasonably determine the circumstances under which their expression would be protected. Far from providing an effective safeguard against prosecutorial overreach, this vaguely formulated defence is likely to intensify the chilling effect on public discourse.

Recommendations:

- Section 16 should be removed entirely. Incidents of stalking and harassment should be addressed under existing criminal laws, and restrictions on expression should only be considered as a matter of last resort and in any event must be consistent with the requirements of legality, necessity and proportionality;
- Any attempt to regulate cyber stalking or cyber bullying should be developed in consultation with a meaningful and representative cross-section of civil society, academics, the technology and media industry and other relevant non-State actors.

Corporate liability

Under Section 18(1)(a), a "body corporate" that commits any offence under the Act may be punished with a fine of up to 50 million shillings.

Section 18(1)(b) renders all "principal officer[s] of the body corporate" liable for the same offence unless they prove the offence was "committed without their consent or knowledge" and that they "exercised such diligence to prevent the commission of the offence that they ought to have exercised" given the "nature of their functions" and "prevailing circumstances." Corporate officers found liable may be fined an amount of up to 5 million shillings and/or imprisoned for up to three years.

ARTICLE 19 is gravely concerned that Section 18 would expose online platforms and their operators or employees to severe criminal sanctions for failing to comply with punitive censorship measures that themselves violate international human rights standards:

- Section 18(1)(a), read with the Bill's prohibition of aiding or abetting "false publications" under Sections 12 and 17, might be broadly interpreted to hold Internet platforms and other websites criminally liable for simply hosting information regarded to be "false, misleading or fictitious." Similarly, these platforms could be held liable for hosting "repeated" communications that "detrimentally affects" another person in violation of Section 16(1)(b);
- Section 18(1)(b) violates the requirement of legal certainty under international law, failing to sufficiently define the actions corporate officers must take in order to avoid criminal liability. In particular, it leaves them in the dark about the due diligence processes that would qualify for immunity from liability;
- The cumulative effect of these provisions would not only compel online platforms and websites to comply with content restriction demands that are themselves suspect under international law, but also incentivize them to err on the side of caution restrict content that is perfectly legitimate or lawful.

Recommendations:

- Sections 16 and 17 should be removed in their entirety; in the alternative, Section 18 should not apply to offences committed under Sections 16 and 17;
- Section 18 should expressly state that internet service providers are exempt from liability with respect to any offence committed by a third party under the Bill when they are acting as mere conduits, or merely performing hosting, caching or information location functions;
- Section 18 should clarify that the Bill does not impose general obligations on internet service providers to monitor the information which they transmit or store, or to actively seek facts or circumstances indicating illegal activity.

Investigative procedures and legal assistance

The remaining sections of the Bill establish investigatory powers and procedures, including procedures for facilitating international mutual legal assistance. While ARTICLE 19 does not conduct an exhaustive analysis of this part of the Bill, it nevertheless raises concerns about certain sections that may unduly restrict the rights to privacy and freedom of expression.

Search and Seizure of Stored Computer Data

Section 23(3)(d) requires any person "possessing knowledge" about relevant computer systems to provide computer data or information necessary to "enable" the execution of a warrant. Section 23(3)(e) permits the issuance of warrants requiring "any person in possession of decryption information" to grant the relevant authorities access to such information as necessary to decrypt data required for an investigation. Section 23(3)(f) also provides the authority to compel third party provision of "reasonable" technical and other assistance for the purposes of executing a warrant.

ARTICLE 19 is concerned that that these provisions are vaguely formulated and may provide law enforcement excessive discretion to compel the disclosure of customer data. In particular, the provisions regarding decryption and technical assistance my require internet service providers to insert security 'back doors' in their products, establish key escrows, store data

locally or facilitate mass collection or analysis of users' communications. These measures are inconsistent with the recommendations of the UN Special Rapporteur of expression, which state that orders to decrypt or otherwise provide government access to private communications must be necessary and the least intrusive means available, based on publicly accessible law, clearly limited in scope focusing on a specific target and implemented under independent and impartial judicial authority.

Recommendation:

- Sections 23(3)(d) through 23(3)(f) should permit warrants compelling decryption, technical assistance and government access to communications and communications data only when such orders are necessary and the least intrusive means available to conduct a specific and legitimate investigation, and focused on a specific target.

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 and East Africa, at henry@article19.org.