Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

REFERENCE:
OL KEN 7/2018

10 July 2018

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolution 34/18.

In this connection, I would like to bring to the attention of your Excellency's Government information I have received concerning the **recently adopted Computer and Cybercrimes Act which includes provisions incompatible with Kenya's obligations to respect, protect and promote the right to freedom of expression**.

According to information received:

On 16 May 2018, the Computer and Cybercrimes Bill (the "Act") was signed into law by the President.

The Act establishes two main categories of offences:

1) Offences related to the mishandling of computer systems or data

2) Offences related to content

Offences relating to the mishandling of computer systems or data

Section 14 of the Act punishes anyone who infringes the security measures of a computer system with the "intent of gaining access" to that system and knowledge that such access is unauthorized.

Section 15 makes it an offence for anyone who violates section 14 with "intent of committing a further offence under any law" or facilitating its commission.

Section 17 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. It is specified that "interception" refers to the "monitoring, modifying, viewing or recording of non-public transmissions of data to or from a computer system". The offence is punishable with a fine of up to 10 million shillings and/or 5 years imprisonment.

Section 21 (1) establishes the offence of "cyber espionage" for the unauthorized access to or interception of "critical" data, databases or "a national critical information".

Section 21(4) 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 of benefitting a foreign state against Kenya.

Section 21(5) 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 of benefitting a foreign state against Kenya.

Section 21 (1) offences are punishable with up to twenty years imprisonment and/or a fine of ten million shillings. Section 21(4) and (5) offences are punishable with a fine of up to five million shillings and/or ten years imprisonment.

Section 25 makes it an offence to intentionally input, alter, delete or suppress computer data, if this results in the creation of "inauthentic data".

Offences related to content

Section 22 makes it an offence to "intentionally publish false, misleading or fictitious data" or "misinform with intent". The penalty is up to 15 million shillings in fines and/or two years imprisonment.

Section 27 makes it an offence for a person to "wilfully and repeatedly" communicate "directly or indirectly" with someone else if they "know or ought to know" that such conduct "is likely to expose those persons to the risk of apprehension or fear of violence" or otherwise "detrimentally affects that person".

Section 32 establishes corporate liability for offences under the Act.

While I do not wish to prejudge the accuracy of these allegations, I am concerned that the Act could be used to chill and penalize the legitimate exercise of the right to freedom of expression. Before explaining our concerns, I would like to reiterate your Excellency's Government's obligations to respect and protect the right to freedom of opinion and expression under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), acceded by Kenya on 1 May 1972.

Article 19(1) of the ICCPR guarantees that all individuals "shall have the right to hold opinions without interference". Article 19(2) of the ICCPR provides that "[e]veryone shall have the right to freedom of expression; this right shall include the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." State Parties have a positive obligation to respect and ensure that

those who "impart information" on matters of public interest enjoy an environment that promotes these actions because a "free, uncensored and unhindered" press is essential to the public's enjoyment of the right to seek, receive, and impart information along with the enjoyment of other ICCPR rights (CCPR/C/GC/34).

The right to freedom of expression under Article 19 may only be restricted in accordance with Article 19(3). Article 19(3) states that restrictions must be "provided by law" and "necessary for respect of the rights or reputations of others" or for the "protection of national security or of public order (ordre public), or of public health or morals." It is not enough that these restrictions on the right to freedom of expression be enacted as domestic laws or regulations in order to satisfy the requirement that they are "provided by law". In order to comply with the requirements of Article 19(3), restrictions on the right to freedom of expression must be sufficiently clear, accessible, and predictable for the public to properly regulate its conduct. Finally, these laws restricting the right to freedom of expression must not confer "unfettered discretion" on those "charged with its execution" (CCPR/C/GC/34). The requirement of necessity implies that restrictions must be proportionate, in particular, they must be "the least intrusive instrument" among those which might achieve the desired result and must be "proportionate to the interest to be protected" (CCPR/C/GC/34) and (A/HRC/17/27). The principle of proportionality "must also take account of the form of expression at issue as well as the means of its dissemination" (CCPR/C/GC/34). The criteria for restrictions online are the same as for those offline.

Regarding restrictions on government criticism and historical facts, the Human Rights Committee has concluded that "all public figures, including those exercising the highest political authority such as heads of state and government, are legitimately subject to criticism and political opposition" (CCPR/C/GC/34). Accordingly, the Committee has also asserted that laws "penaliz[ing] the expression of opinions about historical facts are incompatible with the obligations that the Covenant imposes on States parties in relation to the respect for freedom of opinion and expression" (CCPR/C/GC/34).

The full texts of the human rights instruments and standards outlined above area available at www.ohchr.org and can be provided upon request.

Based on the human rights law and standards discussed above, I am concerned that the Act affords your Excellency's Government broad discretion to unduly penalize individuals for holding or sharing personal opinions, creating a chilling effect on legitimate exercises of the right to freedom of expression.

Vague provisions

The Act falls short of Article 19(3)'s requirement that restrictions on the right to freedom of expression be "provided by law" because many sections of the Act contain vaguely defined terms and enforcement authorities are empowered with "unfettered discretion" to investigate, search and arrest individuals in pursuit of crimes accomplished via digital devices. We are particularly concerned that the cyber espionage sections of the Act criminalize large categories of speech in vague and broad terms. For example, the

Act does not define which databases or infrastructure are considered "critical", providing authorities excessive leeway to prosecute unauthorized data access and interception offences as cyber espionage based on vague criteria. Moreover, the Act does not explain what constitutes a "benefit" to a foreign state. These provisions do little to provide individuals with sufficiently clear, accessible and predictable information to properly regulate their conduct. Instead, such vague language may allow for broad and unpredictable interpretations which could criminalize nearly all forms of legitimate expression. As a result, these provisions may create an environment that has a chilling effect on freedom of expression, and where journalists, academics and human rights defenders may be disproportionately affected.

Content-related offenses

I am concerned that the criminalization of "false, misleading and fictitious data" would effectively provide the authorities the role of determining "truth" in public discourse. This would curtail independent journalism, writers, artists and civic engagement essential to a democratic society. The vague prohibition of "false" and "misleading", is subjective and thus prone to abuse, providing authorities with a pretext to prosecute reporting, criticism or commentary deemed controversial. In particular, the prohibition on "fictitious data" may be broadly interpreted to publish anyone publishing satirical material online.

While I recognize the Government's intention to protect individuals from harassment and intimidation, I am concerned that the wording of section 27 "apprehension of fear of violence" and "detrimentally affects" establishes a very low threshold, threatening to penalize anyone who publishes or reposts content that raises the possibility of violence. In particular, I am concerned that this provision could be used to target reporting and commentary on incidents or patterns of violence connected to government or powerful private actors.

Lack of public interest defenses

The Act does not provide for "public interest" defenses for unauthorized disclosures that nevertheless expose fraud, waste or abuse. The lack of such defenses would heighten the risk that government and private whistle-blowers may be prosecuted, enhancing a chilling effect on critical public disclosures of wrongdoing (A/70/361).

Corporate liability

I am concerned that sections on corporate liability would expose online platforms and their operators or employees to criminal sanctions for failing to comply with punitive censorship measures. Platforms and other websites may become criminally liable for simply hosting information regarded to be "false, misleading or fictitious" or "repeated" communications that "detrimentally affects" another person. This may further incentivize platforms and websites to err on the side of caution to restrict content that is lawful.

As it is my responsibility, under the mandate provided to me by the Human Rights Council, to seek to clarify all cases brought to my attention, I would therefore be grateful for your observations on the following matters:

1. Please provide any additional information and any comment you may have on the above-mentioned allegations

2. Please explain how the Computer and Cybercrimes Act complies with your Excellency's Government's obligations to respect and promote freedom of expression under the ICCPR.

I would like to inform your Excellency's Government that this communication will be made available to the public and posted on the website page for the mandate of the UN Special Rapporteur on freedom of opinion and expression: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/LegislationAndPolicy.aspx

Your Excellency's Government's response will also be made available on the same website as well as in the regular periodic Communications Report to be presented to the Human Rights Council.

While awaiting a reply, I urge that all necessary interim measures be taken to halt the alleged violations and prevent their re-occurrence and in the event that the investigations support or suggest the allegations to be correct, to ensure the accountability of any person(s) responsible for the alleged violations.

Please accept, Excellency, the assurances of my highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression