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

REFERENCE:
OL ZMB 1/2021

16 June 2021

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 43/4.

In this connection, I would like to bring to the attention of your Excellency's Government information I have received concerning « the Cyber Security and Cyber Crimes Law, which was signed into law by the President on 23 March 2021.

I would like to offer the following comments on various provisions of the law, which, if not amended, may restrict the exercise of freedom of expression in ways that are incompatible with article 19 of the International Covenant on Civil and Political Rights (ICCPR), acceded to by Zambia on 10 April 1984, and article 9 of the African Charter on Human and Peoples' Rights.

According to its preamble, the Law seeks to provide for cyber security in Zambia; provide for the protection of persons against cybercrime; provide for child online protection; facilitate identification, declaration and protection of critical information infrastructure; provide for the collection of and preservation of evidence of computer and network related crime; provide for the admission, in criminal matters, of electronic evidence; provide for registration of cyber security services providers; and provide for matters connected with, or incidental to, the foregoing.

I would first like to highlight that article 19 of the ICCPR protects the right of everyone to freedom of opinion without interference. Article 19 of the ICCPR also protects the right to freedom of expression, including the right of everyone to freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, through any media of communication.

According to article 19 (3) of the ICCPR, restrictions on the right to freedom of expression must be "expressly prescribed by law" and necessary "for respect of the rights or reputations of others" or for "the protection of national security or of public order, or of public health or morals". In other words, in order for a restriction to be lawful, it must comply with the requirements of legality, necessity and proportionality and according to an order by an independent and impartial judicial authority, in accordance with due process and appellate review.

In this context, I would also like to recall that the Human Rights Council has previously affirmed that "the rights that individuals enjoy offline must also be protected online" (A/HRC/RES/20/8).

I. ***Limitations to freedom of expression***

Part IX of the law criminalises a number of online speeches that are protected under international law. In particular, article 69 of the Law criminalizes the intentional publication of any electronic communication, "with the intent to coerce, intimidate, harass, or cause emotional distress to a person".

Furthermore, article 54 criminalises the publication of "false, deceptive, misleading, inaccurate" information that intends to "compromise the safety and security of other person". It however leaves the determination of what "false" and "deceptive" information may be to the interpretation of law enforcement officers.

Article 65 also punishes anyone who uses "hate speech" which is broadly defined as "verbal or non-verbal communication, action, material whether video, audio, streaming or written, that involves hostility or segregation directed towards an individual or particular social groups on grounds of race, ethnicity, antisemitism, tribalism, sex, age, disability, colour, marital status, pregnancy, health status and economic status, culture, or religion".

In other parts of the text, the law also refers to terms central to the interpretation of crimes, such as "cyber-attack", "cyber threat" and "corrupt morals", but it fails to define them.

The State has a duty to protect against speeches that meet the threshold of article 19 (3) and article 20 of the ICCPR. However, article 69 of the Law is overbroad and may effectively criminalizes the accessing, sharing and transmitting of information that is essential in a democratic society, including news reporting, criticism of the government and the expression of unpopular, controversial or minority opinions.

It is well established that restrictions to the free circulation of ideas and opinions, including those that may be perceived as offensive, shocking or disturbing the State or a segment of the population, do not comply with the right of everyone to freedom to seek, receive and impart information and ideas. In effect, by obstructing the free flow of information, the government may deprive the population of access to critical knowledge, which is particularly important at a time of a global pandemic and upcoming general elections. I would like to emphasise that the respect for diversity, pluralism and independent information is a necessary condition for the functioning of any democratic society. As a result, I would advise that article 69 is amended to ensure its compliance with international human rights law.

Broadly or vaguely worded restrictions to the freedom of expression are incompatible with the requirement of legality. As emphasised by the Human Rights Committee, it is not enough that restrictions on freedom of expression are formally enacted as domestic laws or regulations. Instead, restrictions must also be sufficiently clear, accessible and predictable (CCPR/C/GC/34 para. 25).

In this context, I would first like to underscore that terms like "hate speech" or "false news" are not a legitimate interest on the basis of which expression may be restricted in conformity with the ICCPR. According to international law, only "advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law" (Article 20 of the ICCPR).

In two different reports on "hate speech and incitement to hatred" submitted to the General Assembly (A/67/357 and A/74/486), my predecessors stressed that "in order to prevent the abuse of hate speech laws [...] only serious and extreme instances of incitement to hatred be prohibited as criminal offences". My predecessors have encouraged States to set high and stringent thresholds, taking into account, inter alia the following elements when restricting speeches incompatible with article 20 of the ICCPR: seriousness, intent, content, scope, likelihood of harm, imminence and harm, imminence and context, which are further elaborated in the Rabat Action Plan on the prohibition of any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (A/HRC/22/17/Add.4, annex, appendix). I would like to encourage your Excellency's Government to draw on these well-established international standards to revise the part of the law related to "hate speech" to ensure its implementation does not unduly restrict the freedom of expression.

Concerning false information, the Human Rights Committee has made clear that the right to freedom of expression applies to all kinds of information and ideas, irrespective of the truth or falsehood of the content (CCPR/C/GC/34 para. 49). The Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda[1] published by my predecessor and regional experts on freedom of expression, including the Special Rapporteur on Freedom of Expression and Access to Information in Africa, sets out the applicable human rights standards in this context. It notably highlights that "General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, and should be abolished".

II. Due process obligations

Part IV (Article 15) of the Law authorizes cyber inspectors to interrogate individuals and compel the production of documents or information based solely on the receipt of "information regarding an alleged cyber security threat or an alleged cyber security incident."

Part V of the Law authorizes the Minister of Information and Broadcasting Services to collect and store what the Minister considers "critical information", which is defined as "any information for the purposes of national security or the economic and social well-being of the Republic". Critical information must be stored on a server or data server located in Zambia, except where special authorization is granted, and must be surrendered to the Ministry "where the purpose for which critical information expires or the data controller ceases to exist" (Article 18).

Article 28 of the law further allows cyber inspectors to obtain a warrant to inspect a computer or information system and make electronic copies of records. Article 29 further authorizes law enforcement officers to intercept electronic communications according to a broad set of grounds that include the mere threat of bodily harm and the possibility that a person may damage property. Furthermore, article 30 authorises law enforcement authorises to compel service providers to intercept communications and/or disclose the sender's location based on there being "reasonable grounds to believe" that it would assist in dealing with an "emergency" involving danger to a person or the fact that "property is likely to be damaged, is

[1] https://www.ohchr.org/Documents/Issues/Expression/JointDeclaration3March2017.doc

being damaged or has been damaged". Only after the request has been made to the service provider must law enforcement officers submit a written confirmation and affidavit to the service provider, as well as a judge, who will determine whether the request was appropriate (Article 30(6)). Service providers are required to use communication systems that support the interception of communications in "realtime and fulltime", with failure to do so leading to a fine of up to five hundred thousand penalty units and/or imprisonment of up to five years (article 38), and must "store call related information" as specified by statutory instrument (article 40(2)). Article 39 requires service providers to obtain the name, address and identity number or business registration information of persons using their services.

The interrogation of individuals and compelled production of evidence, as well as the collection and storage of broadly defined "critical information", without judicial review, raise serious concerns for both the freedom of expression online and the right to privacy. I would like to stress that Article 17 of the ICCPR permits interference with the right to privacy only where it is "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant", is in pursuit of "a legitimate aim" and "meet[s] the tests of necessity and proportionality" (A/69/397, para. 30). It is not enough that the restriction is useful, desirable, or reasonable – it must be "the least intrusive instrument among those which might achieve the desired result" (CCPR/C/GC/34).

I am thus seriously concerned that the introduction of these new broad surveillance powers, without sufficient safeguards, fails to meet the necessity test. The vaguely worded grounds for exercising the powers granted under these articles leaves open the possibility of the arbitrary exercise of executive authority. I am particularly concerned that these broad powers may result in the arbitrary targeting of anyone who may critically report on the government's actions, including journalists, human rights defenders or political opponents. Revising this part of the law seems essential to protect the freedom of expression in advance of the coming general elections.

I would like to underscore that in order to be lawful, restrictions on privacy and expression online need to be necessary and proportionate to achieve one of a small number of legitimate objectives, set forth in Article 19 of the ICCPR. While these principles apply in all cases of targeted surveillance, they have particular force when expression in the public interest is implicated. Targeted surveillance creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information (A/HRC/41/35, para. 26). In this context, the Human Rights Committee has emphasized that restrictions must never be invoked as a justification for the muzzling of any advocacy of multiparty democracy, democratic tenets and human rights (CCPR/C/GC/34 para. 23).

In addition, I am concerned that the Law authorises the interception of communications based on vaguely worded grounds, which could be as minor as previously committed property damage, with only *ex post facto* judicial oversight, and furthermore requires service providers to put in place infrastructure to facilitate the interception of communications. The Law leaves open the possibility for communications surveillance to be authorized on a broad and indiscriminate basis, without the need for "cyber inspectors" to establish the factual basis prior to undertaking surveillance. Furthermore, the burden of proof of "reasonable grounds" to believe that damage to a person or property has, is or will take place, is extremely low

given the "potential for surveillance to result in investigation, discrimination or violations of human rights" (A/HRC/23/40 para. 56).

States are required by Article 17(2) of the ICCPR to regulate, through clearly articulated laws, the recording, processing, deletion, use and conveyance of automated personal data and to protect those affected against misuse by State organs as well as by private parties (A/HRC/17/27). I am therefore concerned by the law's failure to establish sufficient guarantees against abuse, and the lack of clear provisions to protect information gathered as a result of the law, including the length of the storage of such data and their collection by state authorities and private companies.

Furthermore, identity disclosure requirements permit authorities to more easily identify persons, which has the effect of eradicating anonymous expression, which may be particularly important for journalists, human rights defenders, government critics or others who might fear risks of reprisals. Restrictions on anonymity facilitate State surveillance by simplifying the identification of individuals accessing or disseminating content, and facilitate the collection and compilation of large amounts of data by the private sector, which places a significant burden and responsibility on corporate actors to protect the privacy and security of data (A/HRC/23/40).

III. Sanctions

The law provides for severe punishment against those who may contravene with the law. For instance, the offence of "hate speech" entails a minimum fine of up to five hundred thousand penalty units (approximately US$ 6,800) or a prison term of up to two years, or both. The publication of "false information" may result in a fine of minimum five hundred thousand penalty units or a prison term of up to five years, or both. Using or causing a computer to be used for the purposes of "cyber terrorism", defined as "unlawful use of computers and information technology to unlawfully attack or threaten to attack computers, networks and the information stored therein done to intimidate or coerce a government or its people in furtherance of political or social objectives and to cause severe disruption or widespread fear in society" is liable on conviction to life imprisonment (Article 70). Any person convicted of a "cyber attack", which is not defined in the law, may be fined up to five hundred thousand penalty units and/or imprisoned up to five years. Any offence under the law for which a penalty is not specified carries a penalty of up to five hundred thousand penalty units and/or a prison term of up to five years, or a penalty of up to one million penalty units for a body corporate or unincorporate body.

In addition, any person who fails to attend to answer questions or provide documents or information to a cyber inspector is subject to a fine of up to five hundred thousand penalty units or a prison term of up to two years, or both (Article 15(5)).

Furthermore, all offences in the new law are considered "cognisable", which means that they are considered easily identifiable without the need for further investigation. As a result, those suspected of committing them may be arrested without a warrant.

I am concerned that the law creates a number of offences that are vaguely worded, and thus vulnerable to being arbitrarily applied, yet carry the threat of punitive fines and lengthy prison sentences. As highlighted by the Human Rights

Committee, criminal sanctions, in particular imprisonment for expressions that relate to political discourse, commentary on one's own and on public affairs, discussion of human rights, journalism, cultural and artistic expression and religious discourse, are not deemed proportionate with an effective exercise of the right to freedom of expression (CCPR/C/GC/34 para. 11). The Human Rights Committee further stressed that, in assessing the proportionality requirement, the "value placed by the Covenant upon uninhibited expression is particularly high in the circumstances of public debate in a democratic society concerning figures in the public and political domain" (CCPR/C/GC/34 para. 34).

In the light of these observations, I invite your Excellency's Government to continue our dialogue and to provide responses to the abovementioned concerns. I note that this new legislation was adopted at a time of a global pandemic and of general elections to take place in August 2021 where the enjoyment of the freedom of opinion and expression, including the right to receive information, and the right to privacy, will be particularly important for the realisation of several other civil, cultural, economic, political and social rights.

I encourage the Government to take all necessary steps to carry out a detailed review of the Law, to amend the provisions that do not meet international norms related to freedom of opinion and expression and to ensure its implementation does not unduly restrict international human rights law. I stand ready to provide your Excellency's Government with any technical advice it may require in this context.

This communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received from your Excellency's Government will be made public via the communications reporting website within 48 hours. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

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

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