Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association; the Special Rapporteur on the situation of human rights defenders and the Special Rapporteur on the right to privacy

Ref.: OL LBY 3/2022
(Please use this reference in your reply)

31 March 2022

Excellency,

We have the honour to address you in our capacities as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Special Rapporteur on the rights to freedom of peaceful assembly and of association; Special Rapporteur on the situation of human rights defenders and Special Rapporteur on the right to privacy, pursuant to Human Rights Council resolutions 43/4, 41/12, 43/16 and 46/16.

In this connection, we wish to submit **the following comments on the Anti-Cybercrime Law** adopted by the House of Representatives on 26 October 2021. The draft law was adopted only one day after it was included in the parliament's agenda and was passed without prior consultation with experts, civil society organisations or human rights defenders.

We are concerned that the Anti-Cybercrime Law (hereafter "the Law") could have a grave impact on the enjoyment of the right to freedom of opinion and expression and the right to privacy, in particular, both of which are enshrined in articles 19 and 12 of the Universal Declaration of Human Rights (UDHR) and articles 19 and 17 of the International Covenant on Civil and Political Rights (ICCPR), which Libya acceded to on 15 May 1970. The current provisions of the Law are wide ranging in subject matter and pose a detrimental threat to the rights of individuals, residing either in Libya or even outside of the territory, using the internet or other digital technologies, due to the array of provisions and the lack of clear and precise wording.

We also wish to express our concern with regard to the timing of the adoption of the Law and its proximity to the presidential elections on 24 December 2021. It is concerning that such far-reaching provisions on the right to freedom of expression online have been implemented, reportedly in an unprecedentedly quick process and without prior consultation with civil society organisations or experts on the subject matter, in the lead up to the presidential elections. This timing could indicate that the Law may have been passed with expediency in order to be applicable to individuals who express opinions online in relation to the elections. Similarly concerning, is that the draft Law was not made publicly available prior to its tabling in the House of Representatives, nor has a copy of the Law been made publicly available following its adoption.

We encourage the withdrawal of the Law, and to hold extensive, multi-stakeholder consultations with civil society organizations, journalists, human rights defenders and other relevant actors in the process of redrafting a piece of legislation on the issue of Cybercrime, so as to ensure its scope and content are in compliance with your Excellency's Government's international human rights obligations.

The Law has reportedly been drafted with the stated aims of: "helping to achieve justice and information security"; "protecting the public order and public morals"; "protecting the national economy"; "reserving the rights of legitimate usage of modern technologies"; and "reinforcing general trust in the safety and security of electronic transactions".

International Standards

Before providing comments on the Law itself, we would like to make reference to the relevant international standards, in particular the right to privacy and the right to freedom of opinion and expression, which are respectively enshrined in articles 12 and 19 of the Universal Declaration of Human Rights (UDHR) and articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR), which Libya acceded to on 15 May 1970.

We would like to recall that article 19 of the ICCPR protects the right to freedom of opinion without interference, and the right to freedom of expression, including the right of everyone to seek, receive and impart information and ideas of all kinds, regardless of frontiers, through any media of communication. Furthermore, the Human Rights Council has previously affirmed that "the rights that individuals enjoy offline must also be protected online" (A/HRC/RES/20/8).

Pursuant to article 19(1), the right to hold opinions without interference is absolute, and is a right to which no exception or restriction is permitted. Further, all forms of opinion are protected, including opinions of a political, scientific, historic, moral or religious nature. It is incompatible with paragraph 1 to criminalise the holding of an opinion, and similarly, it is in violation of paragraph 1 to harass, intimidate, stigmatize, arrest, detain, put on trial or imprison a person for the opinions they may hold (CCPR/C/GC/34, para. 9).

Article 19(3) of the ICCPR provides that restrictions on the right to freedom of expression must be "expressly prescribed by law", and "necessary" for the "rights and reputations of others" or "for the protection of national security or of public order (ordre public), or of public health and morals". As stipulated by the Human Rights Committee in its General Comment no.34 however, restrictions imposed on the exercise of freedom of expression must not put in jeopardy the right itself, must conform to the strict tests of necessity and proportionality, must be appropriate to achieve their protective function and must be the least intrusive instrument amongst those which might achieve their protective function (CCPR/C/GC/34). We also wish to recall that information and ideas which may shock, offend, or disturb, irrespective of the truth or falsehood of the content, are embraced by the scope of article 19(2), as are expressions which may be erroneous, ill-founded, or indulge in parody or satire (A/HRC/47/25 para. 38).

In accordance with article 20 of the ICCPR, the State have the duty to prohibit propaganda for war and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, violence or hostility. However, any such prohibitions and their provisions initiated by the State must be compliant with the strict limitations stipulated in article 19(3) (CCPR/GC/34 para. 50-52). Whilst we appreciate the right and responsibility of States to restrict expressions which meet the requirements of articles 19(3) and 20 of the ICCPR, we would like to caution against the adoption of overly broad legislation which may result in undue restrictions to

freedom of opinion and expression.

The right to privacy is guaranteed by article 17 of the ICCPR, which states that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". Interference with the right to privacy may only be permitted 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). As established by the Human Rights Committee in its General Comment no.16, national legal frameworks must provide for the protection of this right. Further, article 17 refers directly to the protection from interference with "correspondence", a term that should be interpreted to encompass all forms of communications, both online and offline (A/HRC/23/40, para. 24).

As outlined by a previous Special Rapporteur on the right to freedom of opinion and expression, privacy can be defined as the "presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others free from State intervention and from excessive unsolicited intervention by other uninvited individuals (A/HRC/23/40, para. 22).

The rights to freedom of peaceful assembly and of association are enshrined in articles 21 and 22 of the ICCPR, which recognize the right of peaceful assembly (art. 21) and that "everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests" (art. 22). Article 21 further notes that "no restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others." Article 21 of the Covenant protects peaceful assemblies wherever they take place: outdoors, indoors and online; in public and private spaces; or a combination thereof (CCPR/C/GC/37, para. 6). Moreover, article 20(1) of the UDHR guarantees that "everyone has the right to freedom of peaceful assembly and association."

Further, under article 2 of the ICCPR, States have a responsibility to take deliberate, concrete and targeted steps towards meeting the obligations recognized in the respective Covenants, including by adopting laws and legislative measures as necessary to give domestic legal effect to the rights stipulated in the Covenants and to ensure that the domestic legal system is compatible with the treaties.

General Observations

As mentioned above, international human rights law holds that restrictions to freedom of expression must pursue a legitimate aim, which could be the respect of the rights or reputations of others, to protect national security or the public order (ordre public), or public health or morals, however the restriction must further be both necessary and proportionate to the interest to be protected. Whilst we appreciate your Excellency's Government's obligation to protect the public order of Libya, as stated as one of the aims of the Law, we are concerned that the outlined means to achieve this aim are inconsistent with international human rights law and standards regarding the right to freedom of opinion and expression and the right to privacy.

We are concerned that in its current form, the Law may not meet the legality requirement under international human rights law to restrict the freedom of expression, as the grounds for restrictions included in the Law are not rigorously defined with sufficient precision and do not provide adequate guidance on the circumstances under which content or websites may be blocked, or when an individual's actions or behaviour online may be considered unlawful. In accordance with the requirement of legality under article 19(3) of the ICCPR, it is not sufficient for the restriction on freedom of expression to be enshrined in law, but further, the restriction must be sufficiently clear, accessible and predictable (CCPR/C/GC/34, para 25). The requirement for precision is necessary to allow an individual to enable their conduct accordingly.

Article 3 of the Law provides that the provisions of the law shall apply for any of the offences therein if they have been committed either wholly or in part in Libya, and also if committed wholly whilst outside the territory if it is deemed that the "repercussions and effects" of these offences could be spread in Libya, even if such offences are not punishable in the State in which they were committed. We are concerned by this extra-territorial element of the Law, which provides expansive jurisdiction and allows the Libyan authorities to target any individual, residing in the territory or anywhere else in the world, who it deems to have committed one of the acts included in the Law if it is considered that the "repercussions and effects" of these offences could be spread in Libya, even if such offences are not punishable in the State in which they were committed. Whilst universal jurisdiction may be used to prosecute the most egregious of crimes, for their perceived harm to the international order and the international community, the Law in question does not aim to combat such crimes and so we are concerned that the extra-territorial provision may thus be too wide in scope. Article 3 also appears to violate international norms pertaining to freedom of expression which protect the right to seek, receive and impart information "regardless of frontiers".

According to article 4, the use of the internet and "new technologies" is considered "legitimate and lawful", so long as that "public order and morality" are respected. Therefore, any use of the internet which is deemed to have violated these ambiguous concepts can be deemed illegal.

Article 7 provides that the National Information and Security and Safety Authority (NISSA) – an administrative and technical governmental authority – is permitted to monitor all content published on the internet "and any other technical platform" and enables it to block websites and content if deemed to provoke "racial or regional slurs and extremist religious or denominational ideologies that undermine the security and stability of the society".

Pursuant to article 7, in cases of "security requirement or urgency", no prior judicial order would be required for NISSA to block websites or content it deems to have provoked or seemingly be capable of provoking such slurs or ideologies. The monitoring of electronic messages or conversations not considered a matter of security or urgency would require judicial authorization, however no detail or explanation is provided as to what would qualify as a security requirement or urgent. Neither is any measure for determining how or whether the content would undermine the security and stability of Libyan society outlined in the current law.

In accordance with article 8, NISSA is also granted the ability to censor and block access to all websites and pages which contain materials that it deems to be "contrary to public morality".

Article 9 of the Law criminalizes the use of encryption technologies or tools without the explicit consent of NISSA, stating that "no individual or entity shall produce, possess, provide, market, manufacture, import or export encryption tools without NISSA's permission or authorization". – inhibits the digital safety and security of Libyan citizens, and infringes upon the rights to privacy, and protecting their data and online communication. Further, article 39 criminalizes the production, acquisition, distribution, marketing, manufacturing, exportation or importation of encryption tools or devices, without the authorization or permission from the relevant State authority, with a possible maximum imprisonment sentence of 10 years and a minimum between 50,000 – 150,000 Libyan Dinars.

Article 13 provides that anyone who "intercepts an information system for the purpose of obtaining digital data" will face a minimum six-month imprisonment sentence and a fine of 1,000 – 5,000 Libyan Dinars. Article 47 of the Law states that anyone who "in the interest of himself or others, wiretapped communications through the world wide web or any other electronic means" shall face imprisonment, with a minimum sentence of one year – both of which could amount to journalists being charged under the law for either accessing information or communication with sources, including whistleblowers, in order to report on and share information in the public interest.

Article 21 stipulates that any act of "combining or mixing someone's picture or voice, without their written or online consent, by using the internet or any other digital means with the intent of harming others" is punishable by a minimum one-year prison sentence.

According to article 35, "anyone who is aware of the commission or the attempted commission of any of the crimes stipulated in this law" may face imprisonment.

Pursuant to article 37, anyone who "through the worldwide web or the use of any other electronic means, propagates or publishes information or data threatening public security or peace" in either the State of Libya or "any other State", may be subjected to imprisonment of up to 15 years, in addition to a fine of no less than ten thousand Libyan Dinars.

In consideration of the current articles of the Law, we wish to recall the principle of proportionality, which any restriction on freedom of expression must conform to, in order to be permissible in accordance with article 19(3). As stipulated

by the Human Rights Committee, for a restrictive measure to conform to the principle of proportionality it must be appropriate to achieve its protective function, the least intrusive instrument amongst those which might achieve their protective function, and proportionate to the interest to be protected (CCPR/C/GC/34, para. 34). We are therefore concerned that the current provisions of the Law do not meet these requirements, as it permits the monitoring of online content and activity, the blocking of websites and content and includes disproportionately harsh penalties and fines. We recall that criminal sanctions constitute serious interference with the freedom of expression and are disproportionate responses in all but the most egregious cases, and that resorting to criminal law should be used only in very exceptional circumstances of incitement to violence, hatred or discrimination (A/HRC/47/25).

Overbroad and ambiguous terms

In contravention of international legal standards regarding restrictions to freedom of expression, specifically that such restrictions must be formulated by law and with sufficient precision to allow for individuals to conduct themselves accordingly, the Cybercrime Law is replete with vague, overbroad and ambiguous terms in a number of its articles which may have far-reaching consequences for the enjoyment of the right to freedom of opinion, expression and privacy. Pursuant to General Comment no.34, further to being provided for by legislation, any restriction on freedom of expression must be sufficiently clear, accessible and predictable, with the requirement for precision necessary to allow an individual to enable their conduct accordingly (CCPR/C/GC/34 Para. 25).

In this regard, we are concerned by a number of the articles of the Law in its current form, which are ambiguously worded and therefore difficult to interpret and conduct one's behaviour or actions accordingly when using the Internet or any other "digital technologies", which is in itself unclear. In particular, the need for "public order and morality" to be respected in order for internet use to be considered lawful (article 4); scenarios of "security requirement or urgency" which would allow NISSA to block websites and content with no prior judicial order, in cases where such content may be deemed to provoke "racial or regional slurs and extremist religious or denominational ideologies that undermine the security and stability of the society" (article 7); websites or content may also be censored and blocked by NISSA if considered to be "contrary to public morality" (article 8); and the propagation or publication of information or data which could be interpreted as "threatening public security or peace" (article 37).

The lack of elaboration as to what is included in or meant by the concepts of "public order" or "public morality", risk causing individuals to self-censor whilst using the internet, to mitigate the risk of unknowingly violating either. With regard to public morality, the Human Rights Committee observed that the concept of morals "derives from many social, philosophical and religious traditions; consequently, limitations…for the purpose of protecting morals must be based on principles not deriving exclusively from a single tradition", and that any such limitations must be "understood in the light of universality of human rights and the principle of non-discrimination" (CCPR/C/21/Rev.1/Add.4).

Furthermore, we are concerned by the wording of article 7, which relies on the discretion of NISSA to determine whether websites and content could plausibly provoke racial or regional slurs and extremist religious or denominational ideologies

that could undermine the security and stability of the society. The content may not in fact have caused or provoked, intentionally or not, racial or regional slurs and or extremist religious or denominational ideologies, but apparently must merely meet the low threshold of *possibly* provoking expressions of such sentiments or ideologies. That NISSA's authority to determine whether such expressions could possibly produce such an outcome is seemingly not subject to judicial oversight compounds our concern, as it creates a scenario in which the governmental authority could arbitrarily invoke the article in an unlimited number of circumstances.

In this connection, we are concerned that the vague and broad nature of a number of the above-mentioned provisions of the Law may lead to their discriminate application against journalists, human rights defenders, activists and civil society actors who express dissenting views or publish, share or comment on information about the Government, its policies or actions, with such criticism being liable to interpretation as threatening to "public security or peace" or "public order or morality". Pursuant to General Comment no.34, the penalization of a media outlet, publisher or journalist solely for being critical of the government or the political system espoused by the government can never be considered to be a necessary restriction of freedom of expression (CCPR/C/GC/34 para. 42).

Media freedom

We also wish to express concern that the provisions of the law may impinge media freedom in Libya and the rights of journalists to seek, receive and impart information, including information relevant to the public interest. As stipulated by the Human Rights Committee, laws and provisions relating to national security, such as the Law in question, must be crafted and applied in a manner that conforms to the strict requirements of article 19(3), and therefore may not be invoked to prosecute journalists, amongst others, for having disseminated information of legitimate public interest that does not harm national security (CCPR/C/GC/34, para. 30). As the current provisions of the Law do not provide specific description as to what information or content would constitute as a threat to "public security or peace", or similarly, the "security or stability of society" (articles 37 & 7 of the Law), such information or content is open to interpretation and may be arbitrarily invoked against journalists, human rights defenders, whistleblowers, civil society activists and individuals using the internet.

Furthermore, we fear that some of the Law's provisions, specifically articles 13 and 47, may inhibit journalists from accessing information or communicating with whistleblowers or anti-corruption activists, in order to share information in the public interest, as they would respectively criminalise "interference and interception" and "unlawful wiretapping". As emphasised by the former Special Rapporteur on the right to freedom of opinion and expression in his report to the Human Rights Council on the protection of sources of information and whistleblowers, the legal protection of both sources and whistleblowers rests on a core right to freedom of expression, enshrined in article 19(2) of the ICCPR which emphasizes that the freedom applies to information and ideas of all kinds. Sources and whistle-blowers enjoy the right to impart information, but their legal protection when publicly disclosing information rests especially on the public's right to receive it (A/70/361, para. 5).

With specific reference to article 21 of the Law, which criminalises any act of "combining or mixing someone's picture or voice, without their written or online consent, by using the internet or any other digital means with the intent of harming others", we are concerned that no reference is made to exceptions for political or public figures. This may unduly restrict freedom of expression, including within this right the established understanding that public figures, including those exercising the highest political authority, are legitimately subject to criticism, ridicule or parody. According to the Human Rights Committee, "the mere fact that forms of expression are considered to be insulting to a public figure is not sufficient to justify the imposition of penalties" (CCPR/C/GC/34).

Threat of mass surveillance and the digital safety and security of individuals

We are seriously concerned that the Law in its current form would grant the Libyan authorities far-reaching powers to conduct mass surveillance of individuals using the internet or digital technologies, which would constitute violations of the right to privacy and the right to freedom of opinion and expression and be inconsistent with your Excellency's Governments obligations under international law to uphold and promote such rights. Further, such surveillance would be conducted not only on individuals within the territory of Libya, but also those residing outside of the territory.

According to article 7 of the Law, NISSA would be permitted to "monitor the dissemination and display of information through the world wide web or any other technologies", effectively granting the governmental authority unlimited and unchecked power to monitor any content which is available, transmitted or published online. The scope of this article is of grave concern, as it places no restriction on the content that could be monitored by NISSA, effectively rendering all online content vulnerable to State surveillance.

Article 7 states that "without security requirement and urgency", electronic messages and conversations may only be monitored in cases where NISSA has been granted a judicial order by the competent specialised penal judge. However, the article does not stipulate what information or content in electronic messages and conversations would meet a "security requirement" or the parameters of "urgency", crucially lacking sufficient precision and therefore creating a scenario in which such terms could be broadly applied in order to monitor the electronic messages and conversations of journalists, human rights defenders, lawyers, whistleblowers, activists and individuals. Such a scenario could constitute a profound sanctioning of mass State surveillance and amount to widespread violations of the right to privacy, as well as the right to freedom of opinion and expression.

In the digital age, the right to privacy is often understood as an essential requirement for the right to freedom of expression, and undue interference with individuals' privacy, such as through the use of surveillance technologies and monitoring, can both directly and indirectly limit the free development, flow and exchange of ideas, as well as undermine people's confidence and security on the internet (A/HRC/23/40). The General Assembly has condemned unlawful or arbitrary surveillance and interception of communications as "highly intrusive acts" that interfere with fundamental human rights (see General Assembly resolutions 68/167 and 71/199). Further, in its resolution 73/179, the General Assembly established that "surveillance of digital communications must be consistent with international human

rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise comprehensive and non-discriminatory".

As underlined in his report on the subject of surveillance, the former Special Rapporteur on the right to freedom of opinion and expression cautioned against the detrimental effects of targeted surveillance, as it "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). The Special Rapporteur further emphasised that such self-censorship not only shapes and restricts an individual's exercise of freedom of expression, but also the rights to freedom of association, religious belief, culture and so forth (Ibid, para.26). On formulating national legislation to limit surveillance in accordance with obligations under international human rights law, the former Special Rapporteur noted that surveillance should only be authorized in law for the most serious criminal offences.

We fear that the fundamental right of individuals using the internet to hold an opinion without interference may also be violated, due to the expansive surveillance powers it would grant to the Libyan authorities for monitoring online content and activity. In a previous report to the Human Rights Council, the former Special Rapporteur on the right to freedom of opinion and expression outlined how the mechanics of holding opinions have evolved in the digital age and exposed individuals to significant vulnerabilities as holding opinions is no longer an abstract concept limited to what may be in one's mind (A/HRC/29/32 para. 20). As stated in the report, "Individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods. Civil society organizations likewise prepare and store digitally memoranda, papers and publications, all of which involve the creation and holding of opinions" (Ibid). Online interference with the right to hold an opinion may include efforts of mass or targeted surveillance, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes. As the wording of article 7 does not provide any clarification or detail as to the form the monitoring by NISSA would take, we cannot but assume that in the worst case scenario this could render all online content liable to monitoring.

Our concerns regarding the extensive authority granted to NISSA to monitor online communication and content is aggravated by articles 9 and 39 of the Law, which criminalise not only the use of encryption technologies without NISSA's permission, but also the production, acquisition, distribution, marketing, manufacturing, exportation or importation of encryption tools or devices without permission. Encryption technologies and tools provide individuals with a zone of privacy online to hold opinions and exercise freedom of opinion, expression and belief without arbitrary and unlawful interference or attacks, and are particularly important for journalists, human rights defenders, lawyers and civil society to shield themselves, and their sources, from harassment in hostile, political, social, religious and legal environments (A/HRC/29/32 para.12). As encryption technology is widely considered an enabler of the right to freedom of expression in the contemporary technological environment, restrictions on its use must meet the three-pronged test of legality, pursued for a legitimate aim, necessity and proportionality, however it would appear that the current Law would not meet any of the stated requirements. On

outright prohibitions on the individual use of encryption technology, the former Special Rapporteur on the right to freedom of opinion and expression previously outlined that such bans "disproportionately restrict freedom of expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression, without any particular claim of the use of encryption for unlawful ends" (Ibid para. 40).

Furthermore, by legislating that the use of encryption must be granted by NISSA, this unduly and disproportionately places the burden on individuals exercising their right to freedom of expression, by obliging them to justify their need to use encryption technologies – which for journalists, human rights defenders and others, risks placing them under scrutiny by government authorities and subsequently restricting their ability to carry out their work safely and securely, and impinging on their rights to freedom of opinion and expression and association.

Regarding encryption, we wish to recall the Joint Declaration on Challenges to Freedom of Expression in the Next Decade, 2020, in which my mandate, together with regional freedom of expression experts, emphasised the need to address problems that arise in the context of digital technologies, "including… arbitrary and unlawful surveillance; interference with the use of encryption and anonymity technologies", "within the framework of international human rights law".[1] We also called on Governments to "refrain from arbitrary or unlawful restrictions on the use of encryption technologies".

Taken together, the articles of the Law which grant the monitoring of undefined online content by a governmental authority and the articles which effectively outlaw encryption, could constitute a severe curtailment of the rights to privacy, freedom of opinion and expression, and consequently impede the enjoyment of a number of other civil, political, social and cultural rights.

Blocking access to websites and content

Further to granting authority to NISSA to monitor online activity, article 7 of the Law would also enable NISSA to block websites and content if deemed to provoke "racial or regional slurs and extremist religious or denominational ideologies that undermine the security and stability of the society." Aside from our above-stated concerns in relation to the lack of precision regarding the wording of this article, we express additional concern in relation to the power granted to NISSA to seemingly remove content and block access to websites without any apparent judicial oversight mechanism to hold it accountable. Ineffective procedural safeguards and oversight can only contribute to limiting opportunities for accountability, which can lead to the violation of other human rights. States should refrain from adopting models of regulation where government agencies, rather than judicial authorities, become the arbiters of lawful expression.

Furthermore, in previous reports, the Special Rapporteur on the rights to freedom of peaceful assembly and of association has recognized that digital technology is integral to the exercise of the rights of peaceful assembly and

[1] Joint Declaration on challenges to Freedom of Expression in the Next Decade from the UN and regional experts on freedom of expression, 2020
https://www.osce.org/files/f/documents/9/c/425282.pdf

association.[2] Technology serves both as a means to facilitate the exercise of the rights of assembly and association offline, and as virtual spaces where the rights themselves can be actively exercised.[3] Indeed, such technologies are important tools for organizers who seek to mobilize a large group of people in a prompt and effective manner, and at little cost, and also serve as online spaces for groups of people that are marginalized by society and are confronted with restrictions when operating in physical spaces.[4] The mandate holder has called upon States to ensure that everyone can access and use the Internet to exercise these rights, and that online associations[5] and assemblies[6] are facilitated in accordance with international human rights standards. The Human Rights Council has recognized that although an assembly has generally been understood as a physical gathering of people, human rights protections, including for freedom of assembly, may apply to analogous interactions taking place online.[7]

We also wish to recall that States should only seek to restrict online content pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy, and should refrain from establishing laws that would require the "proactive" monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship (A/HRC/38/35).

We are thus concerned that the granting of power to NISSA to block access to websites and content by article 7 of the Law would be in contravention of the rights to freedom of expression as well as of assembly and of association, not only in relation to the right to share and receive information, but also the right of the public to seek and obtain information as well as to mobilize online, rights of paramount importance, particularly in the current national context of elections.

Concluding observations

In light of the above concerns, we urge your Excellency's Government to review and reconsider the contents of the Cybercrime Law due to the detrimental impact its current provisions are likely to have on the enjoyment of the rights to opinion and expression, the right to privacy, the right to freedom of peaceful assembly and of association, and a number of other human rights. The Law in its current form constitutes an overreach of State authority on the actions and behaviour online of individuals residing in and outside the territory of Libya, and could lead to self-censorship, the stifling of civil society, the deterioration of media freedom, and unlawful mass surveillance in the country. In order to prevent such outcomes and review the Law in accordance with international human rights law, we recommend your Excellency's Government to conduct sufficient public consultation on the issue, including journalists, human rights defenders, civil society organisations and activists. We stand ready to provide support and advice to your Excellency's Government on legislative reform on the subject of disinformation should it be deemed useful.

[2] A/HRC/20/27 and A/HRC/38/34.
[3] A/HRC/29/25/Add.1, para. 53.
[4] A/HRC/35/28.
[5] A/HRC/20/27, para. 52.
[6] A/HRC/29/25/Add.1, para. 34.
[7] A/HRC/41/41, para. 11.

As it is our responsibility, under the mandates provided to us by the Human Rights Council, to seek to clarify all cases brought to our attention, we would be grateful for your observations on the following matters:

1. Please provide any additional information and/or comment(s) you may have on the above-mentioned analysis.

2. Please indicate what measures have been taken to ensure the provisions of the Cybercrime Law are compliant with your Excellency's Government's obligations under international human rights law, in particular articles 19, 12, and 20(1) of the Universal Declaration of Human Rights (UDHR) and articles 19, 17, 21 and 22 of the International Covenant on Civil and Political Rights (ICCPR).

3. With regard to article 7 of the Cybercrime Law, please provide detailed information about the forms of information that may be monitored by NISSA, and further, what is meant by "any other technologies".

4. Please clarify how your Excellency's Government will assess the territorial scope of article 3 and its application outside the territory of Libya.

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 after 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 our highest consideration.

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

Clement Nyaletsossi Voule
Special Rapporteur on the rights to freedom of peaceful assembly and of association

Mary Lawlor
Special Rapporteur on the situation of human rights defenders

Ana Brian Nougrères
Special Rapporteur on the right to privacy