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 and the Special Rapporteur on the right to privacy

Ref.: OL NPL 2/2024
(Please use this reference in your reply)

4 April 2024

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 and Special Rapporteur on the right to privacy, pursuant to Human Rights Council resolutions 52/9, 50/17 and 46/16.

In this connection, we would like to bring to the attention of your Excellency's Government some comments **regarding the new provisions introduced under the National Cyber Security Policy 2023 which appear to limit freedom of expression, peaceful assembly and association, access to information and the right to privacy, in violation of international human rights norms and standards**.

National Cyber Security Policy 2023

In 2021, Nepal's cabinet shared a draft version of the National Cyber Security Policy with a limited number of Civil Society Organisations for consultation. It is reported that the initial draft did not reference human rights.

On 8 August 2023, the cabinet approved a new National Cyber Security Policy. According to a government spokesperson, "the policy addresses the future strategy, working guidelines, objectives and plans relating to cyber security."

While the approved policy's background now acknowledges the 'universal norms of civil rights and the commitment to constitutional fundamental rights' and the 'importance of collaborating with civil society and the private sector', the safeguarding of human rights appears to be vague in the long-term plan, strategy and work plan, and to fail to acknowledge human rights, including fundamental freedoms.

This policy is the latest in a series of recent policy decisions by the Nepalese authorities that seem to limit disproportionately freedom of expression and digital rights in the country.

Clause 11.25 – National Internet Gateway (NIG)

Clause 11.25 of the policy provides for the establishment of a Government owned intranet and a National Internet Gateway (NIG). This provision was not in the initial draft circulated in 2021. The NIG refers to a centralised way of controlling internet traffic and ensuring that all powers to monitor entire web traffic lie with the executive. Officials have stated that the gateway allows the Government to take national cyber security measures of monitoring and blocking potentially malicious traffic and to control cyber-attacks and misinformation.

Clauses 11.64-68 "To build a safe online space through regular monitoring for cyber security"

Clause 11.64 calls for restrictions on the dissemination of "deceptive information" via the internet and social media. Clause 11.65 calls for a prohibition of online services targeting women, children, or gender and sexual minorities. Clause 11.66 calls for "control" of online violence and discrimination. Clause 11.67 calls for a prohibition of the dissemination of content that harms national security, spreads hatred or animosity, online harassment and cyberbullying, harms social and communal harmony, and promotes indecency.

Limitations to freedom of expression, peaceful assembly and association, and the right to privacy

It is our opinion that the establishment of a NIG may pose risks to the fundamental freedoms of individuals, particularly the right to freedom of opinion and expression, the freedom of peaceful assembly and association, and the right to privacy. More specifically, we believe that the provisions of clause 11.25, which establishes the NIG, may be in contravention of international human rights law as it would allow the Government to compile personal information without individuals' consent which may lead to heightened risk of surveillance.

In this regard, we draw your attention to articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR), ratified by Nepal on 14 May 1991.

Article 17 of the ICCPR provides that "1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation and 2) Everyone has the right to the protection of the law against such interference or attacks". Article 17 of the ICCPR also includes the right to the protection of personal data, which, among other things, prevents States from requiring the mass retention of personal data by companies and access to personal data outside of clearly defined circumstances and subject to safeguards. The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law (CCPR/C/GC/16).

Article 19 of the ICCPR provides that "Everyone shall have the right to freedom of expression; this right shall include 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." As interpreted by the Human Rights Committee in its general comment 34 "paragraph 3 [of article 19 of the ICCPR] expressly states that the exercise of the right to freedom of expression carries with it special duties and responsibilities […] However, when a State party imposes restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself […] paragraph 3 lays down specific conditions and it is only subject to these conditions that restrictions may be imposed" (paras. 21 and 22)". We further stress that human rights apply online as well as offline. Human Rights Council resolution 12/16, in this respect, called on States to recognise the exercise of the right to freedom of opinion and expression as one of the essential foundations of a democratic society via every medium, including the Internet.

Article 21 and 22 of the ICCPR protect the rights to freedom of peaceful assembly and the freedom of association respectively. Digital technology is integral to the exercise of these (A/HRC/20/27 and A/HRC/38/34). 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 (A/HRC/29/25/Add.1, para. 53). Such technologies are important tools for organisers who seek to mobilise 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 (A/HRC/35/28). The Special Rapporteur on the rights to freedom of peaceful assembly and association has called upon States to ensure that everyone can access and use the internet to exercise these rights, and that online associations (A/HRC/20/27, para. 52) and assemblies (A/HRC/29/25/Add.1, para. 34) 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 the right to freedom of peaceful assembly, may apply to analogous interactions taking place online (A/HRC/RES/38/11).

With these standards in mind, we note that the NIG gives the Government power to block and disconnect potentially malicious traffic. The current policy may lead to centralising control of all internet traffic in and out of the country through a government appointed operator. The authorities would also gain heightened surveillance and censorship capabilities.

As such, the NIG may not only affect the ability of people in Nepal to exercise their rights to freedom of expression, peaceful assembly and association but could also risk arbitrarily restricting the free flow of information between Nepal and the rest of the world, furthering internet fragmentation. This may have several complex and far-reaching negative consequences for numerous human rights, including but not limited to the rights to freedom of expression, peaceful assembly and association, and the right to privacy in Nepal, and may hamper the openness of the internet system.

We recall that any limitation to the right to freedom of expression must meet the three-part test established by international human rights law, namely the test of legality, necessity and proportionality, per article 19(3) of the ICCPR. Firstly, in relation to the requirement of legality, international human rights mechanisms have already clarified that any limitation must be precisely and clearly provided for in a law (CCPR/C/GC/34, para. 25). The policy does not appear to have the status of a law, thus may fail to meet the legality test. The restrictions must pursue one of the exhaustively enumerated legitimate objectives, namely protection of national security or of public order, or public health or morals. While the policy appears to address cyber security, we note that the protection of cyber security is not listed as one of the limitative grounds for restricting expressions under the ICCPR.

Secondly, restrictions must be necessary and proportionate for the protection of legitimate aims, that is, the restriction must be more than “useful”, “reasonable” or “desirable” (A/HRC/29/32, para. 34). As stated by the Human Rights Committee, the ensuing interference with third parties’ rights must not be overbroad. The Committee observed in general comment No. 27 that “restrictive measures must be appropriate to achieve their protective function and be the least intrusive instrument among those which might achieve the desired result”. Thirdly, measures restricting freedom of

expression must comply with the principle of proportionality, i.e., they must establish a direct and immediate connection between the expression and the threat and must not unduly interfere with other rights of the persons targeted (A/HRC/29/32, para. 35). In the present case, the restrictions may lead to heightened risk of generalized surveillance, which may fail to comply with the necessity and proportionality test.

Similarly, while the rights to freedom of peaceful assembly and of association are not absolute, the freedom to access and use digital technologies for the exercise of these rights should be viewed as the rule, and the limitations as the exception. The general norm should be to permit the open and free use of the internet and other digital tools (A/HRC/23/39, para. 76). Resolution 15/21 of the Human Rights Council makes it clear that to be permissible, restrictions should be 'prescribed by 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' (A/HRC/RES/15/21). Where such restrictions are made, 'States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right' (general comment n°31, para. 6).

In this context, we further refer to a 2019 report, named "Surveillance and human rights" (A/HRC/41/35), which the former Special Rapporteur on the freedom of opinion and expression presented to the Human Rights Council. In this report, he recommended that States purchasing surveillance technologies should take measures to ensure that their use is in compliance with international human rights law. This includes reinforcing national laws limiting surveillance, creating public mechanisms for approval and oversight of surveillance technologies, and ensuring that victims of abuse have domestic legal tools of redress.

Furthermore, clauses 11.64-68 contain vague and overbroad terms that may be used to restrict the publication of information in violation of international standards. We recall that the falsity of information is not a valid ground to restrict freedom of expression or freedom peaceful assembly under international law. In her 2021 report 'Disinformation and freedom of opinion and expression', the Special Rapporteur on freedom of opinion and expression outlined that "the right to freedom of expression applies to all kinds of information and ideas, including those that may shock, offend or disturb, and irrespective of the truth or falsehood of the content. Under international human rights law, people have the right to express ill-founded opinions and statements or indulge in parody or satire if they so wish".[1]

In her Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, which she published together with regional experts on freedom of expression, human rights standards applicable in this context were highlighted. The Joint Declaration notes that general prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news," are incompatible with international standards for restrictions on freedom of expression, and should be abolished" Disinformation may be restricted in certain circumstances only, such as where it causes harm to individual reputation and privacy, or incites violence, discrimination of hostility against identifiable groups in society. However,

[1] A/HRC/47/25

any measures to prevent the dissemination of disinformation must comply with the criteria set out in article 19(3) of the ICCPR. Also, terms such as harming social and communal harmony or promoting indecency are open to interpretation and are not sufficiently precise to meet the legality requirement under international human rights standards.

Furthermore, we note that the policy aims to prohibit any online services targeted against women, children, or gender and sexual minorities, as follows:

> 11.53 Public awareness programmes on cyber security shall be organized targeting the senior citizens, women and children, people with special needs and the civil society.
>
> 11.65 The online services targeted against women, children or gender and sexual minorities shall be prohibited.

The wording is vague as it does not specify which type of services are prohibited, and it may thus be applied in an overly restrictive manner. Any legal provision that aims to maintain blanket prohibition, without mentioning the criteria, impairs the rights to freedom of expression, peaceful assembly and association, and is a violation of one's right to privacy.

In addition, the Strategy seem to fail to identify who will be responsible for enforcing these requirements. Private actors should not be responsible for determining the legality of people's behaviour, nor should Governmental agencies. This is the role of transparent, independent and accountable public authorities such as the judiciary (A/HRC/38/35).

Without public consultation or procurement transparency, there is no guarantee that an effective human rights impact assessment has been carried out on the current legislation. International law and standards require meaningful public consultation through a transparent and inclusive process. In his report A/HRC/32/38, the former Special Rapporteur on the freedom of opinion and expression stressed that "any demands, requests and other measures to take down digital content or access customer information must be based on validly enacted law, subject to external and independent oversight, and demonstrate a necessary and proportionate means of achieving one or more aims under article 19(3) of the International Covenant on Civil and Political Rights." In this case, independent and external oversight may be missing.

Conclusions

We believe that the above-mentioned provisions of the National Cyber Security Policy 2023 would give new powers to the Government to impinge on the rights to privacy and to freedom of expression, peaceful assembly and association in a way incompatible with international human rights law. By means of the NIG, the Government could exercise control over online content and implement unrestricted measures of surveillance and censorship. We urge the Government to revise the current policy, allowing for appropriate public consultation in the process, and ensure that the internet remains a tool to promote and strengthen freedom of opinion and expression, freedom of association and peaceful assembly, participation in public and political affairs, and democracy.

It is our opinion that the new policy appears vague in critical areas and may fail to acknowledge the protection of human rights and fundamental freedoms. We urge your Excellency's Government to provide more details on the provisions under clauses 11.64-68 and 12.5, specifically detailing how the right to privacy and the right to freedom of opinion and expression will be upheld. We urge your Excellency's Government to duly consider the abovementioned comments.

We would be grateful for any observations you may have on the abovementioned comments, especially on how your Excellency's Government intends to ensure compatibility of the new regulations with international human rights norms and standards, highlighted in the present communication.

We recommend that there should be more substantive discussion with all stakeholders and that your Excellency's Government draws upon best practices so that the rights to freedom of expression, peaceful assembly and association, and the fundamental right to privacy can be upheld. Given the wide-ranging impact of this proposed policy on individuals and organisations dedicated to the publication and dissemination of information in Nepal, we urge your Excellency's Government to engage in wider consultations with all relevant stakeholders, including our own mandates, so that the final policy can be brought into line with international human rights standards.

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

Ana Brian Nougrères
Special Rapporteur on the right to privacy