Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Working Group on the issue of human rights and transnational corporations and other business enterprises; the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on the situation of human rights defenders

REFERENCE:
AL BGR 2/2021

22 October 2021

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; Working Group on the issue of human rights and transnational corporations and other business enterprises; Special Rapporteur on the rights to freedom of peaceful assembly and of association and Special Rapporteur on the situation of human rights defenders, pursuant to Human Rights Council resolutions 43/4, 44/15, 41/12 and 43/16.

In this connection, we would like to bring to the attention of your Excellency's Government information we have received concerning the **reported use of the Pegasus spyware developed by NSO Group Technologies (the NSO Group) to surveil, intimidate and harass hundreds of journalists, human rights defenders and political leaders in various countries**. We are writing to your Excellency's Government as information received indicates that NSO Group is domiciled in the territory and/or has operations under the jurisdiction of your Excellency's Government.

The United Nations Special Procedures have previously raised with the NSO Group human rights concerns about its Human Rights and Whistleblower policies (OL OTH 52/2019 and OL OTH 2/2020), and also raised concerns about the use of the Pegasus spyware in July 2019 (AL SAU 10/2019) and August 2021 (OL OTH 211/2021). Although we received a response from the company on 10 December 2019 and 20 September 2021, we remain seriously concerned in light of the information we recently received.

According to the information received:

On 18 July 2021, an international investigation exposing widespread global surveillance of the mobile devices of hundreds of journalists, human rights defenders and political leaders, through the use of the NSO Group's Pegasus spyware, was made public. As a result, access to calls, messages, and other data stored on the device of those affected was reportedly hacked. It is reported that at least 180 journalists from about 20 countries were targeted, including countries in relation to which our mandates have previously raised serious human rights concerns about the state of media freedom and the rights to freedom of expression, and freedom of peaceful assembly and association, the situation of human rights defenders and shrinking civic space in general.

On the day after this information was made public, the NSO Group released a statement in which it made the following remarks: "We would like to emphasize that NSO sells it technologies solely to law enforcement and intelligence agencies of vetted governments for the sole purpose of saving lives through preventing crime and terror acts […]. Our technologies are being used every day to break up pedophilia rings, sex and drug-trafficking rings, locate missing and kidnapped children, locate survivors trapped under collapsed buildings, and protect airspace against disruptive penetration by dangerous drones.” In the same statement, the NSO Group claimed that the report published in the international media was “full of wrong assumptions and uncorroborated theories that raise serious doubts about the reliability and interests of the sources”.

Not only did the company reject the information that had been made public, but it also chose not to disclose the results of any internal probe or human rights due diligence process concerning potential human rights harms that may have been caused or contributed to by the company, or directly linked to its products or services through business relationships. As set out in the United Nations Guiding Principles on Business and Human Rights (UN Guiding Principles)[1], companies have a responsibility under international law to respect human rights throughout their activities and operations.

In order to identify, prevent, mitigate and account for how they address their human rights impacts, companies are expected to conduct regular and ongoing human rights due diligence in consultation with relevant stakeholders, and to make public the results of the human rights due diligence conducted, including in relation to the information that has now been made public (Guiding Principle 21).

In addition, States have an obligation under international law to protect against human rights abuse by business enterprises within their territory and/or jurisdiction, and may be considered to have breached this obligation if they fail to take appropriate steps to prevent, investigate and redress human rights abuses committed by private actors.

While we do not wish to prejudge the accuracy of these allegations, we are deeply worried that the surveillance operations that were recently exposed reportedly used technology to surveil hundreds of journalists, human rights defenders and political leaders, whose role is critical in a democratic society, in violation of their rights to freedom of opinion and expression and to be free from any unlawful and arbitrary interference in their private lives. We also recall that digital technology is integral to the exercise of the rights to peaceful assembly and association, as it serves both the facilitation of the exercise of those rights offline and the creation of virtual spaces where those rights can be exercised.

We are further deeply concerned by the allegations that the Pegasus spyware was supplied to and used by State agencies or by entities that do not have a track record of respecting international human rights standards. We fear that the Pegasus spyware may have been planted onto the devices of journalists, human rights defenders and political leaders with the goal of monitoring, intimidating and possibly silencing them, in contravention of human rights laws and norms. If the allegations are confirmed, the unlawful hacking of numerous cell phones may have contributed to infringing the rights to privacy, liberty and security, and possibly to life, of an extremely high number of individuals, in numerous countries.

[1] A/HRC/RES/17/31, Annex.

You may recall that the previous Special Rapporteur on freedom of opinion and expression called for a suitable legal and policy framework for regulation, accountability and transparency within the private surveillance industry (see A/HRC/41/35, para. 60). We reiterate his call "for a moratorium on the global sale and transfer of private surveillance technology until rigorous human rights safeguards are put in place to regulate such practices and guarantee that Governments and non-State actors use the tools in legitimate ways" (Ibid. para. 66).

In connection with the above alleged facts and concerns, please refer to the **Annex on Reference to international human rights law** attached to this letter which cites international human rights instruments and standards relevant to these allegations.

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 allegations.

2. Please provide information on steps that your Excellency's Government has taken, or is considering to take, to prevent and protect against human rights abuses by business enterprises, and in particular by the products and services of the NSO Group, in line with the UN Guiding Principles. Please provide details on the way the expectation to respect human rights for all companies domiciled within your territory and/or jurisdiction in all their activities was communicated and monitored.

3. Please provide detailed information on the laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights, especially the protection of fundamental freedoms, and how they have been used towards the NSO Group, in line with the UN Guiding Principles. Please also provide information whether your Government is considering to enact any mandatory human rights due diligence legislation.

4. Please provide information about any regulatory measures in place that may give effect to EU Regulation 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, which called upon EU Member States to "consider in particular the risk of them being used in connection with internal repression or the commission of serious violations of human rights and international humanitarian law".

5. Please provide information as to any of the steps not covered by your answers to the above questions that your Excellency's Government has taken, or is considering to take, in line with your international human rights obligations to protect human rights, to ensure that the Pegasus spyware has not been sold to, or used by, States or State agencies that

may violate international human rights norms and standards, including but not limited to violation to the right to privacy.

6. Please provide information about any existing mechanisms for victims or other individuals to report on the adverse human rights impacts linked to business activities, and in particular about the misuse of NSO Group technology and services, and thereby gain access to remedy and redress.

We would appreciate receiving a response within 60 days. Passed this delay, this communication and any response received from your Excellency's Government will be made public via the communications reporting website. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

While awaiting a reply, we 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 our highest consideration.

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

Surya Deva
Chair-Rapporteur of the Working Group on the issue of human rights and transnational corporations and other business enterprises

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

Annex
Reference to international human rights law

In connection with above alleged facts and concerns, we would like to refer to the articles 12, 19 and 20 of the Universal Declaration of Human Rights, adopted by the UN General Assembly on 10 December 1948 (UDHR), and articles 17, 19, 21 and 22 of the International Covenant on Civil and Political Rights (ICCPR), ratified by Bulgaria on 21 September 1970, which guarantee the rights to not be subjected to arbitrary or unlawful interference with one's family or home, to freedom of opinion and expression, and to freedom of peaceful assembly and of association.

Article 17 of the ICCPR protects the right to privacy and provides that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence. In relation to the facts set out above, it is pertinent to recall that the Human Rights Committee affirmed in its Concluding Observations to the report presented by Bulgaria (CCPR/C/BGR/CO/3, para. 22) that, in the context of the right to privacy, the protection of "correspondence" includes telephone communications. The General Assembly also emphasized that unlawful or arbitrary surveillance as a highly intrusive act, which violates the right to privacy and may contradict the tenets of a democratic society' (A/RES/68/167). We also refer to General Assembly's resolution 73/179, which noted 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.

In his report on online content regulations, the Special Rapporteur on the rights to freedom of opinion and expression noted that "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/38/35/Add.2, para. 53). In his report on surveillance and human rights, the Special Rapporteur on the rights to freedom of opinion and expression called upon States to "impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place" (A/HRC/41/35 para. 66).

Concerning the allegations that a large number of human rights defenders have been victim of surveillance as a result of their legitimate work reporting on human rights related issues, we would like to refer your Excellency's Government to the fundamental principles set forth in the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, also known as the UN Declaration on Human Rights Defenders. In particular, we would like to refer to articles 1 and 2 of the Declaration which state that everyone has the right to promote and to strive for the protection and realization of human rights and fundamental freedoms at the national and international levels and that each State has a prime responsibility and duty to protect, promote and implement all human rights and fundamental freedoms.

Furthermore, we wish to refer to article 6 (b) and c) which provide that everyone has the right, individually and in association with others to freely to publish, impart or disseminate to others views, information and knowledge on all human rights and fundamental freedoms; and to study, discuss, form and hold opinions on the observance, both in law and in practice, of all human rights and fundamental freedoms and to draw public attention to those matters.

We would also like to refer to the Human Rights Committee's General Comment No. 37 that recognizes that "[A]lthough the exercise of the right of peaceful assembly is normally understood to pertain to the physical gathering of persons, article 21 [of ICCPR] protection also extends to remote participation in, and organization of, assemblies, for example online" (CCPR/C/GC/37, para. 13). Thus, the Special Rapporteur on the rights to freedom of peaceful assembly and of association has emphasized in various reports the importance of digital technology to exercise the mentioned rights, and in his report on freedom of assembly and association in the digital age, he detailed that those "(…) 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" (A/HRC/41/41 para. 11).

We would also like to highlight the UN Guiding Principles on Business and Human Rights, which were unanimously endorsed in 2011 by the Human Rights Council in its resolution (A/HRC/RES/17/31) following years of consultations involving Governments, civil society and the business community. The Guiding Principles have been established as the authoritative global standard for all States and business enterprises with regard to preventing and addressing adverse business-related human rights impacts. These Guiding Principles are grounded in recognition of:

a. "States' existing obligations to respect, protect and fulfil human rights and fundamental freedoms;

b. The role of business enterprises as specialized organs or society performing specialized functions, required to comply with all applicable laws and to respect human rights;

c. The need for rights and obligations to be matched to appropriate and effective remedies when breached."

It is a recognized principle that States must protect against human rights abuse by business enterprises within their territory and/or jurisdiction. As part of their duty to protect against business-related human rights abuse, States are required to take appropriate steps to "prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication" (Guiding Principle 1). This requires States to "state clearly that all companies domiciled within their territory and/or jurisdiction are expected to respect human rights in all their activities" (Guiding Principle 2). In addition, States should "enforce laws that are aimed at, or have the effect of, requiring business enterprises to respect human rights…" (Guiding Principle 3). The Guiding Principles also require States to ensure that victims have access to effective remedy in instances where adverse human rights impacts linked to business activities occur.

States may be considered to have breached their international human law obligations where they fail to take appropriate steps to prevent, investigate and redress human rights violations committed by private actors. While States generally have discretion in deciding upon these steps, they should consider the full range of permissible preventative and remedial measures.

Business enterprises, in turn, have an independent responsibility to respect all internationally recognized human rights (Guiding Principle 11). They are expected to carry out human rights due diligence in order to identify, prevent, mitigate and account for how they address their impacts on human rights (Guiding Principle 15). Where a business enterprise causes or may cause an adverse human rights impact, it should take the necessary steps to cease or prevent the impact. Similarly, where a business enterprise contributes or may contribute to an adverse human rights impact, it should take the necessary steps to cease or prevent its contribution and use its leverage to mitigate any remaining impact to the greatest extent possible (commentary to Guiding Principle 19).

Furthermore, business enterprises should remedy any actual adverse impact that it causes or contributes to. Remedies can take a variety of forms and may include apologies, restitution, rehabilitation, financial or non-financial compensation and punitive sanctions (whether criminal or administrative, such as fines), as well as the prevention of harm through, for example, injunctions or guarantees of non-repetition. Procedures for the provision of remedy should be impartial, protected from corruption and free from political or other attempts to influence the outcome (commentary to Guiding Principle 25).

The Guiding Principles also recognise the important and valuable role played by independent civil society organisations and human rights defenders. In particular, Principle 18 underlines the essential role of civil society and human rights defenders in helping to identify potential adverse business-related human rights impacts. The Commentary to Principle 26 underlines how States, in order to ensure access to remedy, should make sure that the legitimate activities of human rights defenders are not obstructed. In its recent guidance on ensuring respect for human rights defenders (A/HRC/47/39/Add.2), the Working Group on Business and Human Rights highlighted the urgent need to address the adverse impacts of business activities on human rights defenders. It unpacked, for States and businesses, the normative and practical implications of the Guiding Principles in relation to protecting and respecting the vital work of human rights defenders.