

Mandates of the Working Group on the issue of human rights and transnational corporations and other business enterprises; 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; the Special Rapporteur on the situation of human rights in the Palestinian territory occupied since 1967; the Special Rapporteur on the right to privacy; the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; the Special Rapporteur on trafficking in persons, especially women and children; the Special Rapporteur on violence against women, its causes and consequences and the Working Group on discrimination against women and girls

Ref.: AL ISR 11/2021
(Please use this reference in your reply)

27 December 2021

Excellency,

We have the honour to address you in our capacities as Working Group on the issue of human rights and transnational corporations and other business enterprises; 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; Special Rapporteur on the situation of human rights in the Palestinian territory occupied since 1967; Special Rapporteur on the right to privacy; Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; Special Rapporteur on trafficking in persons, especially women and children; Special Rapporteur on violence against women, its causes and consequences and Working Group on discrimination against women and girls, pursuant to Human Rights Council resolutions 44/15, 43/4, 41/12, 43/16, 1993/2A, 46/16, 40/16, 44/4, 41/17 and 41/6.

In this connection, we would like to bring to the attention of your Excellency's Government information we have received concerning the planting of the Pegasus spyware developed by NSO Group Technologies (the NSO Group) in at least six devices belonging to Palestinian human rights defenders and staff members of Palestinian non-governmental organizations, only two weeks after the designation of these organizations as "terrorist associations" by the Government of Israel.

In a letter addressed to your Government dated 5 August 2021 (ISR 7/2021), several United Nations Special Procedures already raised concerns about reported use of the Pegasus spyware to surveil, intimidate and harass hundreds of journalists, human rights defenders and political leaders in various countries. We regret that at the time of this communication, no response has yet been received to that communication.

The United Nations Special Procedures also previously raised human rights concerns related to the activities of the NSO Group in OTH 211/2011, OTH 2/2020 and OTH 52/2019.

According to the information received:

In November 2021, a forensic peer-reviewed investigation of 75 iPhone devices belonging to Palestinian human rights defenders and employees of civil society organizations revealed that at least six were found to be infected with the spyware, including those of the Director of the non-governmental

organization (NGO) Bisan Center for Research and Development, as well as staff of the NGOs Al Haq and Addameer.

The result of these investigations came out only two weeks after the designation as “terrorist organizations” by Israel Defense Ministry of six Palestinian civil society organizations: Addameer Prisoner Support and Human Rights Association, Al-Haq Law in the Service of Man (Al-Haq), Bisan Center for Research and Development, Defense for Children International-Palestine, the Union of Agricultural Work Committees, and the Union of Palestinian Women’s Committees.

When Pegasus is installed on a person’s phone, an attacker reportedly has complete access to the phone’s entire exchanges traffic, including incoming and outgoing communications, emails, media, microphone, camera, passwords, voice calls on messaging apps, location data, calls and contacts. The spyware also has the potential to activate the phone camera and microphone from distance without the phone owner’s knowledge, and to spy on his or her’s calls, activities and life, professional and private. As such, the spyware not only allows for the surveillance of the target, but also of anyone with whom the target is in contact with, via that device, including all the potentially vulnerable victims they are in touch with, as well as international and national officials, journalists, lawyers and colleagues. “Evidence” can also reportedly be planted into devices infected with Pegasus spyware.

The penetrating and monitoring of the devices of human rights defenders and members of NGOs not only violates the privacy rights of these persons, but their confidential activities as human rights defenders and lawyers, and the countless victims that have potentially been in any sort of contact or communication with them. In this regard, we highlight that privacy functions as a gateway right to the protection of a host of other fundamental rights including non-derogable rights, and violating it amounts to violate numerous other rights.

While we do not wish to prejudge the accuracy of these allegations, we are deeply worried about the reported infiltration of the devices belonging to individuals working with Palestinian non-governmental organisations whose peaceful work seeks to promote freedom and justice, the role of which is critical to any democratic society. The rights violated include the right be free from any unlawful and arbitrary interference in their private lives, the right to freedom of opinion and expression, the right to freedom of assembly and association, the right to freedom of religion and belief, the right to family life, and the right to participate in public affairs. Such level of surveillance undermines also the work and confidentiality of journalists vis-a-vis their sources, and of any human rights investigation for the same reason. It enables access and intrusive surveillance and voyeurism of individual’s intimacy. This is important for all, particularly for women, girls and other individuals who face discrimination, violence and persecution based on their sexual orientation and gender identity.

More generally, the use of this spyware is the epitome of the plethora of technologies already used for the widespread and systematic invasive surveillance of Palestinians, especially but not only, human rights defenders and members of human rights non-governmental organisations, that includes phone and internet monitoring and interception, CCTV, and biometric data collection. Digital technology is integral

to the exercise of the rights to freedom of expression and information, to peaceful assembly and association, as it serves both the facilitation of the exercise of those rights offline and the creation of spaces where they can be exercised and enhanced. Digital technology is essential to the exercise of private life, family life and the access provided by such technologies impinges on the most intimate and sensitive parts of a person's life, and also materially affects the lives of all their family members.

In addition to their obligation to refrain from committing any violations of human rights, States have a positive duty to protect individuals against human rights violations committed by themselves but also by private companies, and this concern primarily the protection of any undue interference with their privacy. One key step to effectively prevent abuse of surveillance technology is for States to require by law that private companies are bound by the same obligation as national actors, of respect to human rights subscribed by that state, domestically and internationally, and are fully accountable for any violation that they may cause, directly or indirectly.

The undersigned Special Rapporteurs note that the interference with an individual's right to privacy is only permissible if it is neither unlawful nor arbitrary.¹ Not to be arbitrary such interference must be reasonable and meet the critical tests of legality, necessity, proportionality and non-discrimination. Such interference by the State in the private sphere must be authorized, clearly regulated with sufficient safeguards to avoid its abuse, and subjected to effective oversight. All individuals subject to electronic surveillance programmes must continue to be treated with dignity. The previous Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism underscored the importance of having clear, comprehensive, and human rights-compatible and rule of law-informed guidance regarding the implementation of any monitoring system including at every stage of data collection, management, usage, sharing and retention, as well as the underlying process for determining the "absolute necessity" of such surveillance. He also emphasized the need for effective, independent oversight, including by establishing or expanding existing oversight bodies, to supervise the implementation of these measures.²

As set out in the United Nations Guiding Principles on Business and Human Rights (UN Guiding Principles)³, States are under an obligation to ensure companies 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 diligence⁴ 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.

¹ A/73/163, para. 10, (a) and (b)

² See Krisztina Huszti-Orbán & Fionnuala Ní Aoláin, *Use of Biometrics Data to Identify Terrorists: Best Practice or Risky Business?* (2020), at 16; A/HRC/14/46, para 34.

³ A/HRC/RES/17/31, Annex.

⁴ A/73/163, para. 10, (a) and (b)

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 which Your Excellency’s Government have not responded yet:

1. Please provide any additional information and/or comment(s) you may have on the above-mentioned allegations.
2. Please provide information on the measures in place to ensure the protection of the right to privacy of the six above-mentioned individuals, as well as of any other person – Palestinian or Israeli - subjected to such spyware surveillance.
3. In particular, please clarify the legal and procedural framework in place, the process by which such surveillance is authorized, the oversight mechanism that monitors it;
4. Please clarify how such intrusive surveillance is legal, necessary, proportional and non-discriminatory to its purpose;
5. Please provide information on steps that your Excellency’s Government has taken, or is considering to take, to prevent and protect individuals and groups subjected to its jurisdiction 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 the State of Israel territory and/or jurisdiction in all their activities was communicated and monitored.
6. Please provide information about the regulatory oversight conducted by the Defense Export Controls Agency of the Israeli Ministry of Defense in the context of the following statements made by the NSO Group in its first annual transparency and responsibility report (June 2021): “The Defense Export Controls Agency of the Israeli Ministry of Defense strictly restricts the licensing of some of our products and it conducts its own analysis of potential customers from a human rights

perspective” (page 4); the Defense Export Controls Agency of the Israeli Ministry of Defense “has, in fact, in quite a few cases, denied our applications for export licenses” (page 30).

7. 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.
8. Please indicate what measures have been taken to ensure that human rights defenders, including civil society organizations and activists, can operate in an enabling environment and can carry out their legitimate activities without fear of harassment, stigmatization or criminalization of any kind.
9. Please provide information as to any other steps your Excellency’s Government has taken, or is considering to take, in line with your international human rights obligations to protect human rights.
10. 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.

This communication and any response received from your Excellency’s Government will be made public via the communications reporting [website](#) within 60 days. 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.

Given the gravity of the practices described in this letter, which have the potential to undermine the entire edifice of human rights that protect all persons against the invasion by the State of their privacy, we may be considering to publicly express our concerns in the near future, as we believe that the general public should be informed about the existence of technologies, practices and threats to their rights that concern each of us. While the information at hand appears to be reliable, we would welcome an early response from your Excellency’s Government to this letter. Any public expression of concern on our part will indicate that we have been in contact with your Excellency’s Government’s to clarify the issue in question.

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

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

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

Michael Lynk
Special Rapporteur on the situation of human rights in the Palestinian territory
occupied since 1967

Ana Brian Nougrères
Special Rapporteur on the right to privacy

Fionnuala Ní Aoláin
Special Rapporteur on the promotion and protection of human rights and fundamental
freedoms while countering terrorism

Siobhán Mullally
Special Rapporteur on trafficking in persons, especially women and children

Reem Alsalem
Special Rapporteur on violence against women, its causes and consequences

Melissa Upreti
Chair-Rapporteur of the Working Group on discrimination against women and girls

Annex

Reference to international human rights law

In connection with above alleged facts and concerns, we would like to refer to the articles 12 and 19 of the Universal Declaration of Human Rights, adopted by the UN General Assembly on 10 December 1948 (UDHR), and articles 17 and 19 of the International Covenant on Civil and Political Rights (ICCPR), ratified by Israel 3 October 1991, which guarantee the rights to not be subjected to arbitrary or unlawful interference with one's family or home and to freedom of opinion and expression.

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.

In addition, the Special Rapporteur on the rights to peaceful assembly and 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 like to reiterate to your Excellency’s Government’s obligations through the ratification of the International Covenant on Discrimination against Women (CEDAW) in 1991, in particular Article 7 which provides that States shall take all appropriate measures to eliminate discrimination against women in the political and public life of the country, including the right to participate in non-governmental organizations and associations concerned with the public and political life of the country. In this context, we also wish to recall that the Committee on the Elimination of Discrimination against Women in its General Recommendation No. 19 (1992), updated by General Recommendation No. 35 (2017), defines gender-based violence against women as impairing or nullifying the enjoyment by women of human rights and fundamental freedoms, and constitutes discrimination within the meaning of article 1 of CEDAW, whether perpetrated by a State official or a private citizen, in public or private life. We would also like to refer to CEDAW General recommendation N.38 on trafficking in women and girls in the context of global migration. We would like to reiterate to your Excellency’s Government’s obligations through the ratification of the International Covenant on Discrimination against Women (CEDAW) in 1991, in particular Article 7 which provides that States shall take all appropriate measures to eliminate discrimination against women in the political and public life of the country, including the right to participate in non-governmental organizations and associations concerned with the public and political life of the country. In this context, we also wish to recall that the Committee on the Elimination of Discrimination against Women in its General Recommendation No. 19 (1992), updated by General Recommendation No. 35 (2017), defines gender-based violence against women as impairing or nullifying the enjoyment by women of human rights and fundamental freedoms, and constitutes discrimination within the meaning of article 1 of CEDAW, whether perpetrated by a State official or a private citizen, in public or private life.

As stressed by the Working Group on discrimination against women and girls in one of its reports to the Human Rights Council (A/HRC/23/50), stigmatization, harassment and outright attacks are used to silence and discredit women who are outspoken as leaders, community workers, human rights defenders and politicians. Women defenders are often the target of gender-specific violence, such as verbal abuse based on their sex, sexual abuse or rape; they may experience intimidation, attacks, death threats and even murder. Moreover, in her 2018 thematic report, the Special Rapporteur on violence against women (A/HRC/38/47) stressed that encryption and anonymity, separately or together, create a zone of privacy to protect freedom of expression and to facilitate the freedom to seek, receive and impart

information and ideas, regardless of frontiers. Anonymity online is an important role for women and others at risk of discrimination and stigma, in that it allows them to seek information, find solidarity and support and share opinions without fear of being identified. This holds particularly true for individuals who face discrimination and persecution based on their sexual orientation and gender identity.

In a joint declaration, the Working Group on discrimination against women and girls emphasised that women human rights defenders face unique challenges, driven by deep-rooted discrimination against women and stereotypes about their appropriate role in society. Today's rising fundamentalisms of all kinds and political populism, as well as unchecked authoritarian rule and uncontrolled greed for profit-making further fuel discrimination against women, intensifying the obstacles facing women human rights defenders. In addition to the risks of threats, attacks and violence faced by all human rights defenders, women human rights defenders are exposed to specific risks, such as misogynistic attacks, gender-based violence (including sexual violence), lack of protection and access to justice as well as lack of resources.

We would also like to refer to General Assembly resolution 68/181, adopted on 18 December 2013, on the protection of women human rights defenders. Specifically, we would like to refer to articles 7, 9 and 10, whereby States are called upon to, respectively, publicly acknowledge the important role played by women human rights defenders, take practical steps to prevent threats, harassment and violence against them and to combat impunity for such violations and abuses, and ensure that all legal provisions, administrative measures and policies affecting women human rights defenders are compatible with relevant provisions of international human rights law.

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.

The Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism recalls that any restrictions on the rights to freedom of opinion and expression, freedom of peaceful assembly and association, and privacy on counter-terrorism grounds must comply with the objective criteria of legality, proportionality, necessity and non-discrimination under international law, including by being least intrusive means capable to achieve a

legitimate aim (ICCPR, arts. 17, 19, 22; A/69/397, para 30). States shall not invoke national security as a justification for measures aimed at suppressing opposition or to justify repressive practices against its population (A/61/267, para. 20).

We would also like to highlight the report of the Special Rapporteur on trafficking in persons, especially women and children to the Human Rights Council in 2018, (A/HRC/38/45). In this context we would like to recall the Special Rapporteur's recommendation in paragraph 71 calling on States to ensure that organizations and individuals who assist people on the move are not criminalized or otherwise punished for doing so. We would like to highlight Article 9(3) of the Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, ratified by your Excellency's Government on 23 July 2008, specifies cooperation with non-governmental organizations, other relevant organizations and other elements of civil society, in actions to prevent trafficking in persons. We would like to refer to the OHCHR Recommended Principles and Guidelines on Human Rights and Human Trafficking (2002), Guideline 5(9) encouraging law enforcement authorities to work in partnership with nongovernmental agencies in order to ensure that trafficked persons receive necessary support and assistance.

The Council of Europe Convention on Action against Trafficking in Human Beings, which your Excellency's Government ratified in September 2021, sets important obligations aimed at improving the protection of victims of trafficking.