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.: AL THA 1/2023
(Please use this reference in your reply)

19 April 2023

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, 50/17, 43/16 and 46/16.

In this connection, we would like to bring to the attention of your Excellency's Government information we have received concerning the alleged presence of the Pegasus spyware, developed by the private corporation, NSO Group Technologies (the NSO Group), in devices belonging to at least 35 human rights defenders, academics, political leaders, civil society actors and activists during the height of nationwide demonstrations from 2020 to 2021 in Thailand.

According to the information received:

On 24 November 2021, Apple issued an alert message to the devices of at least 17 individuals, warning that their devices were "compromised by a state-sponsored attacker."

On 18 July 2022, an international forensic investigation team revealed that the phones of at least 30 individuals had been infected by the spyware from October 2020 to November 2021, with increased frequency during the period of political protests across Thailand. The targets of such surveillance were activists, artists, academics, civil society actors and human rights defenders who have made public criticisms of the government and engaged in peaceful demonstrations.

Among those targeted are members of non-governmental organizations working on human rights promotion and protection in Thailand, including the director of the Cross-Cultural Foundation and staff members of iLaw. Out of the 30 individuals, 12 of them are men and 13 are women. The identities of the remaining five remain anonymous.

On 21 July 2022, a member of parliament from the Move Forward Party (MFP) further revealed during a parliamentary debate that the devices of five more individuals, including three key members of the MFP and two leaders of the political group Progressive Movement (PM), had also been infected by Pegasus spyware from December 2020 to August 2021. Out of the five individuals, three of them are male and two are female. Both the MFP and PM are opposition political parties that have been vocal opponents of the government and are actively engaged in campaigns on political and human

rights issues in Thailand. The same forensic investigation of the 30 members of civil society also verified and confirmed the infection of the devices of these additional five individuals.

Apart from this digital surveillance, many of the 35 human rights defenders are reportedly subjected to harassment or criminal charges due to their involvement in peaceful demonstrations.

After the information regarding the Pegasus spyware was made public, government leaders appear to have responded with inconsistent explanations. On 19 July 2022, the Minister of Digital Economy and Society stated in parliament that he was aware that Thai authorities had been employing the spyware to obtain electronic data for the protection of national security and suppression of narcotics. However, the Minister did not refer to any specific government agency using the spyware.

On 21 July 2022, the Prime Minister reportedly denied any knowledge of the spyware. On the same day, the Deputy Minister of Defence reportedly stated that the government did not have any policy on using the spyware or undertaking any other measures that infringe on individual rights. On 22 July 2022, the Minister of Digital Economy and Society reportedly denied that his earlier statement confirmed the use of the spyware in Thailand, claiming that he only knew of the system and did not acknowledge that such surveillance is practiced in Thailand.

On 15 and 22 September 2022, civil society organizations, along with the individuals whose devices have been infected by the spyware, filed a complaint at the lower house of the Thai parliament's Committee on Political Development, Mass Communications, and Public Participation and the National Human Rights Commission of Thailand respectively. However, at the date this communication is sent, both entities have not made any progress in investigation the alleged use of the spyware.

On 15 November 2022, eight of the affected individuals jointly filed a civil lawsuit against the NSO Group at the Ratchadapisek Civil Court in Bangkok demanding financial compensation for the use of the spyware against them. According to the information received, on 21 November 2022, the Court dismissed the lawsuit citing the lack of evidence demonstrating each co-plaintiff shares "a common interest in the subject matter of the case", which is a legal requirement for filing a joint civil lawsuit under section 59 of the Civil and Commercial Procedure Code.[1]

At the time this communication was finalized, the Government has reportedly not taken any effective measures to protect those allegedly subjected to unlawful surveillance.

The following cases reportedly illustrate the presence of Pegasus spyware in Thailand:

[1] Court document on record with Amnesty International, 21 November 2022

Mr. Yingcheep Atchanont

Mr. Yingcheep Atchanont is a prominent human rights defender in Thailand working on key legal issues related to civil and political rights. He works as the programme manager at iLaw, a non-profit organization advocating for legal reforms for the protection of freedom of expression, association, and peaceful assembly in Thailand. Mr. Atchanont led iLaw's campaign for initiating a public-led constitutional amendment to enhance constitutional protection of human rights and the rule of law. Mr. Atchanont's name appeared on a 'watch list' released by the MFP on 9 August 2021, which was allegedly from the Immigration Division of the Royal Thai Police. According to the findings of the forensic investigation mentioned above, Mr. Atchanont's phone was infected by the Pegasus spyware at least ten times from November 2020 to December 2021. It is believed that this infection was in retaliation to his legitimate work in defence of human rights.

Ms. Panusaya Sithijirawattanakul

Ms. Panusaya Sithijirawattanakul is a student and prominent political activist and human rights defender affiliated with the United Front of Thammasat and Demonstration. She led many protests from 2020 to 2021 during which she publicly called for equality, freedom of expression, and the reform of the monarchy. Due to her activism, Ms. Sithijirawattanakul currently faces multiple criminal proceedings, including ten charges under article 112 of the Thai Criminal Code (governing lèse-majesté) for allegedly criticizing the monarchy.[2] Her name also appeared on the 'watch list' that was allegedly from the Immigration Division of the Royal Thai Police.[3] According to the findings of the forensic investigation, Ms. Sithijirawattanakul's phone was infected by the Pegasus spyware at least four times between June and September 2021. It is believed that these infections were as a result of her legitimate work in defence of human rights.

Ms. Puangthong Pawakapan

Ms. Puangthong Pawakapan is a human rights defender and an Associate Professor at Chulalongkorn University's Faculty of Political Science. Her recent research focuses on the Thai military's internal security affairs, including army-sanctioned surveillance of political dissidents and mass organizations. Ms. Pawakapan has been involved in a fact-finding mission on the government's crackdown on the Red Shirt protests in 2010 and coordinated a campaign for the amendment of article 112 of the Thai Criminal Code (governing lèse-majesté) in 2011. In July 2014, Ms. Pawakapan was interrogated by nine male officers from various security agencies regarding her human rights activities. According to the findings of the forensic investigation, Ms. Pawakapan's phone was infected by the Pegasus spyware at least five times from May to July 2021. These infections are believed to have been in response to her human rights driven campaigning and research.

[2] https://tlhr2014.com/archives/40378
[3] https://ilaw.or.th/node/5964

Ms. Bencha Saengchantra

Ms. Bencha Saengchantra is a member of the parliament from the MFP. Ms. Saengchantra plays a leading role in scrutinizing the Thai government's budget expenditure, including spending related to the monarchy. She is also an active advocate for the right to freedom of expression and peaceful assembly and has spoken on various platforms in support of improved human rights protection particularly against arbitrary detention. According to the forensic investigation, Ms. Saengchantra's phone was infected by the Pegasus spyware at least three times from June to July 2021.[4]

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 the measures in place to ensure the protection of the rights to privacy, to freedom of expression and to freedom of peaceful assembly of the 35 above-mentioned individuals, as well as any other person in Thailand, subjected to spyware surveillance.

3. Please provide detailed information as to the legal and factual grounds for the alleged use of the spyware against the above-mentioned individuals. If the above allegations are accurate, please indicate how you have ensured such activities comply with international human rights standards.

4. Please clarify the steps taken to investigate the use of Pegasus spyware and provide information on the plan that your Excellency's Government has 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 on Business and Human Rights.

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

6. Please provide information on steps taken by your Excellency's Government to ensure that human rights defenders and civil society

[4] https://freedom.ilaw.or.th/node/1090

actors are able to carry out their work, including online, without fear of surveillance or any other intimidation, threats or reprisals in a safe and enabling environment.

7. Please provide detailed information concerning measures which are taken to prevent human rights violations being perpetrated by members of the security forces, and which ensure that they are not subjected to surveillance.

We would appreciate receiving a response within 60 days. Past 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

Clément 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

Annex

Reference to international human rights law

The rights to freedom of expression and opinion, as well as of peaceful assembly and of association are guaranteed by articles 17, 19, 21 and 22 of the International Covenant on Civil and Political Rights ("ICCPR"), which was acceded to by Thailand on 29 October 1996.

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.

Article 19(1) of the ICCPR protects the right to "hold opinions without interference." Article 19(2), which protects the right to freedom of expression, states that this right shall include the "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 [or her] choice." Under article 19(3), any restrictions on freedom of expression must be "provided by law", proportionate, and necessary for "respect of the rights and reputations of others", "for the protection of national security or of public order, or of public health and morals". The General Assembly, the Human Rights Council and the Human Rights Committee have concluded that permissible restrictions on the Internet are the same as those offline.

Article 19(3) establishes a three-part test for permissible restrictions on freedom
of expression:

A. Restrictions must be provided by law. Any restriction "must be made accessible to the public" and "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly." Moreover, it "must not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution."

B. Restrictions must only be imposed to protect legitimate aims, which are limited to those specified under article 19(3). The term "rights...of others" under article 19(3)(a) includes "human rights as recognized in the Covenant and more generally in international human rights law."

C. Restrictions must be necessary to protect legitimate aims. The requirement of necessity implies an assessment of the proportionality

> of restrictions, with the aim of ensuring that restrictions "target a specific objective and do not unduly intrude upon the rights of targeted persons."[15] The ensuing interference with third parties' rights must also be limited and justified in the interest supported by the intrusion. Finally, the restriction must be "the least intrusive instrument among those which might achieve the desired result.

The former Special Rapporteur on the rights to freedom of opinion and expression submitted a report on surveillance and human rights in which he highlighted the rights affected and threats posed by targeted surveillance on the work of human rights defenders and journalists, and 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 articles 21 and 22 of the ICCPR which protect the rights to freedom of peaceful assembly and of association. In order to be effective, these rights must be exercised free from any forms of intimidation or harassment of any sort.

The rights to freedom of peaceful assembly and of association are further enshrined 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. The Declaration provides that everyone has the right, individually or in community with others, to assemble peacefully, to form governmental or non-governmental organizations (article 5). It also states that everyone has the right to engage in peaceful activities to counter violations of human rights and fundamental freedoms (article 12).

Furthermore, given that many of the victims of this surveillance are human rights defenders, we deem it appropriate to remind you of the important and legitimate role that human rights defenders play and the protection they are entitled to by international law. We wish to highlight in particular the Declaration on the Rights and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms also known as the Declaration on Human Rights Defenders, and which states 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 the primary responsibility and duty to protect, promote and implement all human rights and fundamental freedoms.

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.