United Nations A/HRC/51/NGO/143

General Assembly

Distr.: General
6 October 2022

English only

Human Rights Council
Fifty-first session
12 September–7 October 2022
Agenda item 5
Human rights bodies and mechanisms

Written statement* submitted by Maat for Peace, Development and Human Rights Association, a non-governmental organization in special consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[20 August 2022]

* Issued as received, in the language of submission only.

Misusing Technology to Engage in Acts of Reprisals

Preamble

Maat for Peace, Development and Human Rights has noted the growing dependence on technology by United Nations member states, their agents and companies operating under the laws of these countries, which has led to the misuse of this technology in some cases to engage in acts of bullying, reprisals, and intimidation of human rights defenders, political oppositions, and individuals working in civil society. The abuse also extended to persecuting these groups to suppress their voices and impose restrictive challenges on their work. In a related context, Maat denounces the objections made by some member states about the participation of civil society in the ongoing discussions to formulate a final draft of an agreement on combating the use of information and communications technology for criminal purposes, an agreement that is supposed to be designed to redress the victims of reprisals resulting from the misuse of technology. Maat requests that the Ad Hoc Committee for Adoption of the Convention broaden the base of participation of civil society, the private sector, and all relevant stakeholders.

First: Use of spyware to threaten human rights defenders

Using spyware against journalists and human rights defenders is a violation of a wide range of basic rights, including the right to freedom of opinion, expression and information. Illegal surveillance is also a violation of the right to privacy guaranteed by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

Reliable reports revealed that out of the fifty thousand mobile phones that were attacked by filtering “zero-click”, one of the tools of the Pegasus program (1), 180 of them belonged to human rights defenders and journalists (2), For more understanding of the seriousness of this tool, once the spyware reaches a mobile phone or computer, it can access passwords, calls, contacts, emails, search logs on websites, geographical location, even encrypted communications, and can activate access to the phone’s camera and the microphone. The program can be installed by connecting to the target device, and once connected; the target device is subjected to hacking without warning (3).

A number of countries in the Middle East and Southeast Asia have used these programs to intimidate human rights defenders, and imprison them for long periods of time.

In Israel, in June 2022, an Israeli court extended the administrative detention of a French lawyer of Palestinian origin (R.H) for another three months, or what is known as administrative detention, until September 2022. An Israeli military court had sentenced the latter to administrative imprisonment in March 2022 on charges related to membership in the Popular Front for the Liberation of Palestine, and other charges of endangering the security of the region (4), but he rejected all the of them. Earlier and prior to his detention, (S.H) complained to Israel about the alleged use of the surveillance company Pegasus spyware NSO Group to gain illegal access to his mobile phone, he was one among other Palestinian activists whose phones have been hacked (5). In Thailand, 24 political activists, three academics, and three members of civil society groups were targeted and their mobile phones hacked between October 2020 and November 2021 using the same program (6).

In Qatar, the Migrant Workers' Rights Defender (MB) is still afraid of revealing his identity even after leaving Qatar. The latter was hacked on the internet by the State Security Service in the State of Qatar. At the end of April 2021, an unknown person sent him a link of an NGO report on the rights of migrant workers. Once he accessed the link, which was not working, he was hacked, and this led to revealing his identity to the party that hacked him, which later turned out to be the Qatar State Security (7). A week after his phone was hacked; the latter was arrested, specifically on May 4, 2021, by people in the Qatar State Security, and was subjected to solitary confinement incommunicado for more than a month, in contravention of the United Nations Standard Minimum Rules for the Treatment of Prisoners. He was interrogated by the State Security for three consecutive days, and the Qatari Public Prosecution charged him with fabricating and publishing false news with the aim of

endangering public regime in Qatar (8). He was released in June 2021 with a large fine estimated at 25 thousand Qatari riyals, equivalent to 6900 US dollars. He was only able to leave Qatar on August 16, 2021, after an international organization paid him the fine. (9)

Second: Complicity of technology companies with governments in reprisals

As governments engage in various violations of online freedom of opinion and expression and the right to privacy, using spyware, tech partnerships are equally implicated in a range of violations of the same rights, and the practices of such companies as Instagram, Facebook, TikTok and others run counter to their stated values and with the principles they are supposed to abide by in terms of users and popular content on its platforms (10).

For example, in May 2022, some former Instagram content managers, in Farsi language, revealed that the Iranian intelligence offered them money ranging from 5,000 to 10,000 in order to delete the accounts of journalists and human rights defenders, and reliable reports stated that the Islamic Republic of Iran mainly targeted the deletion of the account of the human rights defender and media. (M.a.e.n). In light of the recent protests led by Iranian citizens, some opposition bloggers in the Islamic Republic of Iran noticed that the Instagram platform had deleted specific videos criticizing the policies of the Supreme Leader of the Islamic Revolution in the Islamic Republic of Iran (11).

In a related context, Facebook deleted Palestinian content on its platforms (Facebook, Instagram), w here deleting content opposed to Israel was not a coincidence, but was based on a previous agreement between the Israeli government and Facebook, an agreement that resulted in the establishment of a monitoring team aimed at changing what is known as content inciting violence, according to the two concepts of terrorism and incitement stipulated in the agreement. However, the definition of the two concepts was based on a purely Israeli point of view, which illustrates the company’s clear bias against Palestinian content (12).

“Facebook” did not only delete posts considered by the previously prepared artificial intelligence algorithms as an attack on Israel, “Facebook “ also deleted many accounts for Palestinian and Arab bloggers and Palestinian activists who criticize Israel and criticize civilian casualties in Gaza due to Israeli missiles. Although the Meta company, which is the owner of Facebook, has acknowledged the existence of errors and the consequent recommendation of the company's monitoring board to conduct an independent investigation, but the results of the investigation have not yet been announced (13).

Third: The United Nations convention on cybercrime

In 2019, the United Nations General Assembly voted under Res. 74/247/ to establish a specialized committee to develop a convention on combating the use of information and communication technologies in cybercrimes (14).

The committee should facilitate the hearing of the voices of independent human rights defenders whose rights, especially digital rights, have been violated.

Maat also believes that there is an urgent need for the initial draft of the agreement to take into account the national laws in the member states, so that some countries do not take it as a pretext not to ratify the agreement or even to ratify it with reservations.

Maat, therefore, recommends the following:

- Member States should develop a draft resolution to stop the global selling, transfer and use of monitoring technology that are misused to undermine human rights;
- Upping pressure in order to hold the technological companies that sell spyware technologies for governments accountable, due to their human rights violations;
- Social media companies must stop adopting a double standard policy in dealing with the popular content on their platforms;

- The specialized committee need to develop an agreement on combating the use of information and communications technology in committing online crimes and to ensure broader participation of civil society organizations and private sector entities in formulating the final draft of the draft agreement.

---

1. https://bit.ly/3zUfmx1
2. https://bit.ly/3dnOQo9
3. https://www.occrp.org/en/the-pegasus-project/how-does-pegasus-work
4. https://bit.ly/3bQZIKV
5. Ibid
6. https://bit.ly/3dnQru9
7. https://www.migrant-rights.org/wp-content/uploads/2021/08/Malcolm-Bidali-Statement-8-19.pdf
8. https://bit.ly/3w1MDoT
9. Ibid
10. https://bit.ly/3dtTGQS
11. https://ecfr.eu/publication/iron-net-digital-repression-in-the-middle-east-and-north-africa/
12. https://bit.ly/3ibI4lF
13. https://bit.ly/3w3g222
14. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement