assemblea

UNREPRESENTED NATIONS & PEOPLES ORGANIZATION
unpo.org

Barcelona, April 28th, 2022

To the attention of: United Nations Special Rapporteurs
Office of the High Commissioner on Human Rights

Ms. Irene Khan	Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.
Mr. Clément Nyaletsossi Voule	Special Rapporteur on the rights to freedom of peaceful assembly and of association.
Ms. Mary Lawlor	Special Rapporteur on the situation of human rights defenders.
Mr. Fernand de Varennes	Special Rapporteur on minority issues.
Ms. Elżbieta Karska	Working Group on the issue of human rights and transnational corporations and other business enterprises.

Subject: The Spanish Government's Use of NSO Group's Pegasus Spyware to Surveil Catalonia's Self-Determination Movement

Dear UN Special Rapporteurs,

The Assemblea Nacional Catalana (ANC) and Unrepresented Nations and Peoples Organization (UNPO) wishes to bring to your attention recent revelations made public on the Kingdom of Spain's concerning the use of cyber-surveillance technology (Pegasus Spyware) to undermine and repress Catalonian civil society. In particular, we would like to report the cases of six individuals, all members of Assemblea Nacional Catalana (ANC) – members of the UNPO since 2018 – that have been confirmed via independent digital forensic analysis as targets of Pegasus spyware: Elisenda Paluzie, Jordi Sànchez, Arià Bayé, Sònia Urpí, Jordi Domingo Ceperuelo, and Jordi Baylina.

The Spanish state's disregard for the Catalan people's fundamental rights have been ceaselessly demonstrated in recent years, particularly following the 2017 Referendum on the Independence of Catalonia. The recent Pegasus revelations exposed by Citizen Lab epitomizes, yet again, the diminishing state of civil and political liberties in Spain. The ANC and UNPO are deeply concerned over these latest developments, and wishes to emphasize the necessity of holding governments accountable where satisfactory evidence of their unwarranted deployment of cyber-surveillance technology to surveil, intimidate, and harass human rights defenders can be attributed.

The submission is comprised of this letter and a report published on 18 April 2022 by Citizens Lab – enclosed, as well as accessible online at https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ – presenting new independently verified evidence on the use of NSO Group's Pegasus spyware by the Kingdom of Spain against a

significant number of Catalan politicians, activists, journalists as well as their family members in some instances.

Pegasus Spyware

Pegasus spyware is a sophisticated surveillance tool permitting operators to read text messages (including encrypted messages), listen to voice calls, track location, examine photos and browsing history, as well as enabling remote access to the device's microphone and camera. NSO Group, the Israeli-based company that develops and sells the surveillance technology, claims Pegasus technology is strictly sold to government client only. The Pegasus spyware has reportedly been linked to political surveillance in (45) countries.[1]

Citizen Lab, a digital rights research group based at the University of Toronto, in collaboration with civil society organizations has been at the forefront of large-scale investigations into how governments are using NSO Group's spyware to monitor and silence human rights defenders, journalists, and other civil society actors. These attacks target specific users and typically take the form of (1) zero-click exploits, which do not require the target to click on a link or surf a malicious website to be infected, and (2) malicious SMSes, which typically take the form of sophisticated personalized messages reflecting a detailed understanding of the target's habits, interests, activities, and concerns (e.g., fake news updates, or texts purporting to come from national tax authorities, etc.)

The human rights abuses linked to the use of NSO Group's highly intrusive Pegasus technology have been well documented in recent years.[2] Governments using such spyware on individuals not only impede their right to privacy but also their rights to freedom of expression and association. These rights are enshrined in international law by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, UN Human Rights Committee documents, and the UN Guiding Principles on Business and Human Rights, as well as regional instruments that similarly oblige States to protect individuals from targeted surveillance such as the African Commission on Human and Peoples' Rights and the Inter-American human rights system. Given the technology's extremely deep level of intrusion, international human rights norms posit that their use can generally only ever be justified in the context of investigations into serious crimes and grave security threats.

Crucially, the unchecked use of Pegasus surveillance technologies is liable in generating a considerable chilling effect on the legitimate activity of civil society, particularly as it relates to those defending citizen's rights and rule of law. Consequently, deployment of the technology risks contributing to an increasingly shrinking space for civil society and human rights work worldwide, while rapidly exacerbating digital threats against human rights defenders both online and offline.

An array of United Nations human rights actors, including the UN High Commissioner for Human Rights, have repeatedly raised serious concerns about the dangers of authorities using surveillance tools from a variety of sources supposed to promote public safety in order to hack the phones and computers of people conducting legitimate journalistic activities, monitoring human rights

[1]Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, "Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries" *Citizen Lab,* 18 September 2018. Available at: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[2]Pegasus project, amnesty, citizen lab, etc. "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally" *Amnesty International,* 18 July 2021. Available at: https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/.

or expressing dissent or political opposition.[3] On multiple occasions throughout 2021, UN Special Rapporteurs have sent Joint Allegation Letters to governments in which NGO Group is domiciled or holds operations under its jurisdiction, related specifically to the use of Pegasus spyware to surveil, intimidate and harass hundreds of journalists, human rights defenders and political leaders in various countries.[4] Strong condemnation has similarly come from the European Union, with investigations recently launched by the European Parliament, as well as from the Inter-American Commission on Human Rights, who in March 2022 held a hearing on the abuse of Pegasus spyware in El Salvador.[5]

The United Nations, along with support from more than 150 human rights organizations, have also called for a much-needed global moratorium on the sale, transfer and use of such surveillance technology until robust regulations are guaranteed.[6]

However, despite mounting evidence of the technology's integral capacity to abuse and violate fundamental human rights, most States have yet to earnestly address the problem, while Governments around the world who have deployed the technology against its citizens continue to enjoy impunity.

Targeting of Catalan's Pro-Self-Determination Organizations

The April 2022 report by Citizen Lab, in collaboration with Catalan civil society groups, confirms at least 63 individuals targeted or infected with Pegasus spyware. The hacking covers a spectrum of civil society in Catalonia, from academics and activists to non-governmental organizations (NGOs). A number of confirmed victims of Pegasus hacking also provided forensic artifacts from their devices to technical experts with Amnesty International's Security Lab, which independently examined and confirmed the report's findings.

Reports that Spanish intelligence services had the spyware program Pegasus at their disposal had already been speculated for several years. In July 2020**,** joint investigations led by El País and The Guardian showed that phones of the former president of the Catalan regional parliament, Roger Torrent, and former regional deputy and minister, Ernest Maragall, had been targeted with Pegasus spyware.[7] In 2020 it was also reported that other pro-independence actors received notice from Whatsapp and Citizen Lab that their devices had been targeted, including Jordi Domingo, a pro-independence activist and member of the Assemblea Nacional Catalana (ANC)*,* as well as former regional MP Anna Gabriel, a leading figure in the Catalan independence movement who had fled to

---

[3]Office for the High Commissioner for Human Rights, "Use of spyware to surveil journalists and human rights defenders Statement by UN High Commissioner for Human Rights Michelle Bachelet" *OHCHR*, 19 July 2021. Available at: https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner?LangID=E&NewsID=27326.

[4]See: Israel JAL ISR 7/2021 and JAL ISR 11/2021; Cyprus JAL CYP 3/2021; Bulgaria JAL BGR 2/2021.

[5]Amnesty International, "El Salvador: Hearing on abuse of Pegasus spyware to be held by Inter-American Commission on Human Rights" *Amnesty International,* 15 March 2022. Available at: https://www.amnesty.org/en/latest/news/2022/03/elsalvador-pegasus-iachr/.

[6]Amnesty Int. et al, "Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology" *Amnesty International,* 27 July 2021. Available at: https://www.amnesty.org/en/documents/doc10/4516/2021/en/.

[7]Stephanie Kirchgaessner, Sam Jones, "Phone of top Catalan politician 'targeted by government-grade spyware", *The Guardian,* 13 July 2020. Available at: https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware ; Joaquín Gil, "Catalan parliamentary speaker's cellphone was targeted with a spy program only available to governments", *El País*, 14 July 2021. Available at: https://english.elpais.com/politics/catalonia_independence/2020-07-14/catalan-parliamentary-speakers-cellphone-was-targeted-with-a-spy-program-only-available-to-governments.html.

Switzerland over fears she would not receive a fair trial on charges related to her involvement in the 2017 independence referendum.[8]

The April 2022 Citizen Lab revelations, however, reveals a significantly greater web of victims associated with the Catalan independence movement, with almost all of the incidents occurring between 2017 and 2020 (i.e., the time period leading up to and following the October 2017 Catalan independence referendum).

The report reveals the extensive list of victims, targeted either directly with Pegasus, or via suspected relational targeting, to include: every Catalan Member of the European Parliament (MEP) that supported independence; every Catalan president since 2010 either while serving their term, before, or after their retirement; a wide range of legislators from at least five Catalan political parties; lawyers representing prominent Catalans; as well as multiple Catalan civil society organizations that support Catalan political independence, including five members of the Assemblea Nacional Catalana (ANC). A number of spouses, siblings, parents, staff, or close associates of primary targets were also revealed to have been targeted.

Despite conclusive evidence of members of the Catalan pro-independence movement being surveilled via Pegasus – a technology *only* available to state's - Spain's National Intelligence Centre (CNI) have so far refused to respond to specific questions about the alleged use of NSO Group spyware, while the Interior Minister has publicly denied having relations with NSO or having acquired Pegasus.

While Citizen Lab cannot conclusively attribute the targeting to a specific government, the findings conclude that a range of circumstantial evidence points to a strong nexus with the Kingdom of Spain. This is because (1) the targets were of obvious interest to the Spanish government; (2) the specific timing of the targeting matches events of specific interest to the Spanish government; (3) the use of bait content in SMSes suggests access to targets personal information, such as Spanish governmental ID numbers, (4) Spain's CNI has reportedly been an NSO Group Customer, and Spain's Ministry of Interior reportedly possesses an unnamed but similar capability; and (5) it unlikely that a non-Spanish Pegasus customer would undertake such extensive targeting within Spain, particularly in light of the serious diplomatic and legal repercussions for a non-Spanish government entity.

Assemblea Nacional Catalana (ANC) Victims

Assemblea Nacional Catalana (ANC), is a grassroots organization that brings together around 100,000 people from all parts of Catalan society (local, national and international). The Assembly makes active efforts to defend Catalans' rights, denounce the oppression endured by them and peacefully promote the right of self-determination and the aspirations of the Catalan community as to their political future. The ANC has been a target of repression by the Spanish authorities on multiple occasions, particularity during and following the organization of the 2017 referendum.

The October 1st 2017 referendum on the independence of Catalonia saw participation of 2,2 million people (43% turnout), with the "Yes" to independence gaining 90% (2,044,038 votes) of the votes cast. In response to the referendum, Spanish authorities sent thousands of troops of the National Police and Guardia Civil to Catalonia, the latter which is a police body under the authority of the

[8]Stephanie Kirchgaessner, Sam Jones, "Phone of top Catalan politician 'targeted by government-grade spyware", *The Guardian,* 13 July 2020. Available at: https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware.

Ministry of Defense. The police actions included hunting for ballot boxes, mail, posters and flyers promoting the participation in the referendum. Masses of paperwork and postal mail were reported and confiscated, which ultimately could not be counted. The response of Spanish National Police and the Spanish Civil Guard was also excessively violent, and widely condemned by human rights organizations worldwide for the disproportionate levels of police brutality imposed.[9]

Following these events, former ANC President and later Catalan Parliament Speaker Carme Forcadell was imprisoned in relation to the organization of the peaceful referendum - in her case for allowing a debate in Parliament. Another former ANC President, Jordi Sánchez, was imprisoned for calling for peaceful protests on September 20th 2017, and was not freed until June 2021 following a government pardon. During the organization of the referendum, many ANC members were also harassed by Spanish paramilitary Guardia Civil, with ANC promotional materials commandeered and taken away. The website of the ANC was also attacked with content taken down, while the Spanish authorities have also prosecuted and fined the ANC with egregious penalties for campaigns encouraging networking and promotion of Catalan businesses.[10]

The April 2022 Citizen Lab report revealed multiple ANC members to have been targeted with Pegasus. The victims, whose devices had been positively verified via independent digital forensic analysis, include the following six individuals:

1. <u>Elisenda Paluzie: 4 confirmed attacks.</u>

<u>Profile:</u> Professor Elisenda Paluzie (ANC President, 2018 – 2022) is a prominent Catalan economist, academic, and activist. Prior to her role with the ANC, she served as dean of the Faculty of Economics and Business at the University of Barcelona.

<u>Date(s) and Circumstances of Attacks:</u> Ms. Paluzie first discovered that her phone had been hacked in June 2018 after taking her phone to an IT security expert who discovered spyware on the device. Following this Ms. Paluzie regularly got her mobile phone analyzed for spyware and she changed it regularly. In November 2019 another compromise was discovered, confirmed to be Pegasus spyware and she changed her mobile again. In August 2020, Ms. Paluzie was informed by Citizen Lab that two SMSes she had received were Pegasus attacks (May and June 2020). In March 2022 Citizen Lab checked also her former mobile phone from 2019 and confirmed an infection on or around October, 29th, 2019. Amnesty International's Security Lab peer reviewed forensic evidence first identified in the Citizen Lab investigation related to October 29th 2019 targeting and infection of Ms Paluzie's phone, and found evidence[11][12].

<u>Political Context</u>: The attacks coincided with her first election as president of the ANC in March 2018, the period after the sentence of the Catalans leaders in 2019, and her reelection as President of the ANC in June 2020. Some of the SMSes purported to be a news story about the ANC. On June 10, 2020, as she was running for a board seat with ANC and as online voting began, a second infection attempt arrived. It masqueraded as a Twitter update from a Catalan newspaper on the elections to the ANC board.

---

[9]Human Rights Watch, "Spain: Police Used Excessive Force in Catalonia" *Human Right Watch,* 12 October 2017. Available at: https://www.hrw.org/news/2017/10/12/spain-police-used-excessive-force-catalonia.

[10]Assemblea National Catalana, "Assemblea" Available at: https://int.assemblea.cat/assemblea/.

[11] Spain: EU must act to end spyware abuse after prominent Catalans targeted with Pegasus https://www.amnesty.org/en/latest/news/2022/04/spain-pegasus-spyware-catalans-targeted/

[12] Appendix E – Pegasus Forensic Traces per Target Identified in the Aftermath of the Pegasus Project Revelations https://www.amnesty.org/en/latest/research/2021/08/appendix-e-pegasus-forensic-traces-per-target-identified-in-the-aftermath-of-the-revelations-of-pegasus-project/

2. Jordi Sànchez: 25 confirmed attacks.

Profile: Jordi Sànchez (ANC President, 2015 – 2017) is a prominent Catalan political activist and former President of the ANC. In October 2017 he was imprisoned, accused of sedition in connection with the Catalan independence referendum, while in October 2019 was sentenced to 9 years imprisonment. The arbitrary pre-trial detention, excessive penalty and overall judicial harassment perpetrated by the Spanish authorities received widespread condemnation from international human rights groups, before receiving a government pardon in June 2021.

Date(s) and Circumstances of Attacks: Mr. Sànchez first had checks undertaken on his mobile phone while he was in prison. Mr. Sànchez was first seen targeted with a Pegasus SMS infection attempt via SMS 2015, shortly after a large demonstration in Barcelona. On April 20, 2017 Mr. Sanchez was targeted the day prior to the Catalan government meeting with civil society groups to speak on the October referendum. On October 1, 2017 Mr. Sanchez received a message stating a police "offense" was starting months after polls opened. Another infection identifies occurred on October 13, 2017, just days before his arrest. Forensic labs confirmed Mr. Sanchez was infected at least four times between May and October 2017. Between 2017 and 2020, Mr. Sànchez received at least 25 more Pegasus SMSes, most of which masqueraded as news updates relating to Catalan and Spanish politics. He also received messages purporting to come from the Spanish tax and social security authorities.

Political Context: The attacks, which started in 2015, coincide with Mr. Sànchez initial appointment as President of the ANC. This is the earliest Pegasus infection attempt that Citizen Lab observed as the bulk of the targeting uncovered occurred between 2017 and 2020. As seen, messages received by Mr. Sànchez often coincided with important political events, such as Catalan government meetings and public demonstrations. **The SMSes targeting his phone in 2020 coincided with days when he was given weekend release from jail.**

3. Arià Bayé: 1 confirmed attack.

Profile: Arià Bayé is a pro-independence activist and has been a Member of the General Board of the Catalan National Assembly since 2018. He was prosecuted in 2017 after a student's demonstration in favor of a reduction of university fees ("La Pública a Judici"). The trial was held in July 2021, and he was acquitted. In the period 2019-2020, he was responsible for political relations of the Catalan National Assembly. He is the youngest victim in this case. He was 26 at the time of the attacks.

Date(s) and Circumstances of Attacks: Mr. Bayé was attacked during the beginning of the Covid-19 pandemic. Upon being advised to check his phone for particular kind of SMSes, Mr. Bayé found two or three texts with similar characteristics as Pegasus attacks. One SMS, dated on May, 14th 2020, has been confirmed by Citizen Lab to have been a Pegasus attack.

Political Context: In March 2020, just before the lock-down due to the Covid-19 pandemic, Mr. Baye had meetings with CUP, Òmnium Cultural, and other social movements to organize solidarity networks to deal with the pandemic among socially vulnerable groups. In April 2020, Mr. Baye had meetings with candidates at the elections to the General Board of the Catalan National Assembly, with members of the board of the Òmnium Cultural and of Poble Lliure (one of the parties that is member of the CUP).

4. Sònia Urpí: 2 confirmed attacks

Profile: Sònia Urpí has been a Member of the General Board of the Catalan National Assembly since June 2020. Ms. Urpí is the partner of Jordi Baylina, a communications expert linked to the exile who had suffered 26 attacks. In July 2020, she became responsible for mobilizations at the Catalan National Assembly and organized the 11th September (Catalan's National Day) peaceful pro-self-determination demonstration.

Date(s) and Circumstances of Attacks: In July 2020 Ms. Urpi had her phone checked for spyware shortly after her partners phone had been found hacked Ms. Urpi's phone was then discovered to have been attacked on or around June 22, 2020, just after ANC board elections in May. Two attacks have been confirmed around this time period (June 2020).

Political Context: The attacks coincide with Ms. Urpí's joining of the civil society organization, Assemblea National Board, after she was elected to the role on June 13, 2020. Both attacks took place after the elections during the week of June 22, 2020. Amnesty International's Security Lab, confirmed both attacks stemmed from Pegasus infections and targeting.

5. Jordi Domingo Ceperuelo: 1 confirmed attack.

Profile: Jordi Domingo is a technical agricultural engineer currently working in the field of education. He is a Catalan pro-independence activist, having been an active member of the Catalan National Assembly since 2015. He has held responsibilities as a member of the ANC's local board in the town of Reus. He actively participated in the October 2017 Catalan self-determination referendum, in which he took part in the peaceful, non-violent defense of polling stations in the face of violent attacks by Spanish riot police officers. He is the president of the Observatory of Catalanophobia.

Date(s) and Circumstances of Attacks: Upon Citizen Lab detecting a weakness through a security breach with Whatsapp, Mr. Domingo was contacted and informed in October 2019 that he had been identified as affected by a Pegasus spyware attack. An official confirmation was also provided by Whatsapp. The attack is reported to have occurred in May 2019.

Political Context: The attacks coincide with activities of an organization Mr. Domingo presided over, in which they requested the time and space to demonstrate in Plaça de Sant Jaume at the same time the JUSAPOL (anti-independence police union). The dates of the attack also coincide with the Council of the Catalan Republic's submission of application under Article 155 (ousting of the Catalan government) and the Catalan referendum for independence.

6. Jordi Baylina: 26 confirmed attacks

Profile: Jordi Baylina is the technology lead at Polygon, a popular decentralised Ethereum scaling platform, who supports the Catalan cause. He is also an advisor on projects related to digital voting and decentralisation, and has built a widely-used privacy toolkit.

Date(s) and Circumstances of Attacks: Mr. Baylina was extensively attacked, receiving at least 26 infection attempts, and 10 times infected between October 2019 and July 2020. Mr. Baylina was one of the most attacked targets. Mr. Baylina was infected at least eight times via SMSes between October 2019 and July 2020. Those dates included on or around: June 6, 2019 and July

11, 2019, October 29, 2019, November 15, 2019, November 26, 2019, December 11, 2019, December 23, 2019. One such text message masqueraded as a boarding pass indicating the operator had access to Baylina's Passanger Name Record (PNR). Another message sent to Jordi Baylina included a portion of his actual official tax identification number, suggesting that the Pegasus operator had access to this information. Mr. Baylina was also targeted with infection attempts masquerading as a tweet from European NGO European Digital Rights and a tweet purporting to be the Swiss telecom provider Swisscom.

Political Context: Infection attempts against Mr. Baylina began after the sentencing of the Catalan leaders, which sparked protests across Catalonia.

In light of the fact these attacks generally took place during crucial decision-making periods, particularly during and after the referendum, attribution of responsibility to the Spanish authorities and the underlying motives appear self-evident – that is, a vividly clear political impetus to weaken and undermine a fully democratic movement advocating for the right to self-determination. It should be noted that, while the right to self-determination does not grant an automatic right to independent statehood of any peoples who seek it, the right to believe in and seek independent statehood through non-violent and lawful means is protected under international human rights law.

In this regard it is necessary to recall that, according to NSO Group, Pegasus spyware is provided only to authorized governments for the purpose of helping them combat terror and crime. In fact, NSO Group has published sections of contracts which require customers to use its products only for criminal and national security investigations.[13] Crucially, the above-mentioned victims were not committing any form of terrorism or serious crime when targeted. To the contrary, they were carrying out perfectly legitimate and lawful activities, well within the normal exercise of their rights to political opinion, participation in public life, and freedoms of expression, association and assembly.

The Spanish state's deployment of Pegasus technology to a fully democratic, peaceful movement advocating for their people right to self-determination demonstrates Spain's increasing intolerance towards the Catalan people and their expressed political aspirations. The criminalization of dissenting opinions as it relates to the Catalan self-determination movement moreover indicates Spain's total disregard of its legal obligation to protect the rights of the Catalan people and, in particular, their collective right to self-determination as enshrined in Article 1 of the UN Charter, the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR).14

Diminishing Civil and Political Liberties in Catalonia

Following Citizen Lab's revelations that NSO Group's Pegasus was (highly likely) used by actors within the Government of Spain against civil society, and specifically those advocating for Catalonian self-determination, the ANC and UNPO are deeply concerned by the diminishing of civil and political liberties observable in Spain.

[13]Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani and Michael Safi, "Revealed: leak uncovers global abuse of cyber-surveillance weapon" The Guardian, 18 July 2021. Available at: https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.

[14]Article 1 of the ICCPR and ICESCR read: "All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development".

These revelations represent a continuation of long-standing and systematic repression against the Catalan minority. Over the past decade, but particularly in the years since the 2017 referendum, citizens in Catalonia have witnessed a marked deterioration of human rights. Freedoms of press, speech, opinion, association and assembly, the rights to liberty and security of persons, and the right to a fair trial have all been weakened as the Spanish state has attempted to quash Catalonian self-determination.

The imprisonment of elected representatives and civil society leaders of the Catalan pro-independence movement following the 2017 referendum on charges such as sedition have, in particular, been widely criticized by UN bodies and human rights organizations alike for their damaging interference on freedom of expression, association and assembly. Aside from making political prisoners out of Catalan politicians who advocated a peaceful and democratic self-determination process, the increasing criminalisation of political dissent in Spain, particularly as it relates to the Catalan self-determination movement, have led to the arrests of academics, journalists, community activists and other public figures who have expressed divergent political opinions.

The country's so-called "gag law" introduced in 2015 and highly criticized by UN Special Rapporteurs and human rights groups alike,[15] continue to be another major area of concern – allowing authorities the ability to fine journalists and media organizations for distributing unauthorized images of police, strictly limit demonstrations, and impose disproportionately heavy fines on offenders. Moreover, during the most recent Universal Periodic Review (UPR) of Spain in January 2020, 22 member states also expressed their concerns on the deterioration of the rights of peaceful assembly and freedom of expression in the country since 2015.16

Institutionalized Surveillance by Spanish Authorities

Prior to the Pegasus revelations, accusations of the Spanish state's use of espionage against political opponents had frequently emerged. Spain's willingness to turn to highly invasive technologies, often without proper judicial oversight, as a regular means of gathering information on citizens raises serious concern over the credibility of the country as a democratic, human rights abiding nation. For instance:

- In 2001, the Spanish Ministry for Interior purchased the Sistema integral de interpretación de las comunicaciones (SITEL), spyware the Guardia Civil and CNI used to track suspects' phones.[17] The purchase was heavily criticized for impeding on the right to privacy, not least because it could be employed to access personal data such as Documento Nacional de Identidad without judicial authorization.
- In 2010, the CNI and National Police were reported to have paid at least 209,000 euros to the Milan-based surveillance software company Hacking Team for use of its spyware.[18]

[15]UN Special Procedures, "Two legal reform projects undermine the rights of assembly and expression in Spain - UN experts" OHCHR, 23 February 2015. Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15597&LangID=E.

[16]See: UN Human Rights Council, Universal Periodic Review Spain, Matrix of Recommendations https://www.ohchr.org/en/hr-bodies/upr/es-index.

[17]RTVE, "SITEL, el polémico sistema del Gobierno para "pinchar" llamadas" *RTVE,* 5 November 2009. Available at: https://www.rtve.es/noticias/20091105/sitel-polemico-sistema-del-gobierno-para-pinchar-llamadas/299414.shtml.

[18]Ximena Villagrán, "El CNI pagó más de 200.000 euros a Hacking Team para espiar móviles" *El Confidencial*, 6 July 2015. Available at: https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/.

The purchase was first revealed in 2015 when WikiLeaks published internal Hacking Team emails, of which the CNI confirmed its purchase of the spyware.

- In 2015, the Citizen Lab mapped the proliferation of Finfisher, a sophisticated computer spyware suite sold exclusively to governments for intelligence and law enforcement purposes, and identified a suspected Spanish customer.[19]
- In 2018 Belgium's intelligence services were reported to have launched an investigation to address claims that Spanish authorities had deployed a number of secret agents and placed a GPS transmitter under the car of former Catalan president Carles Puigdemont.[20]
- In 2019, it was reported that the Spanish intelligence service, the CNI, has been conducting illegal surveillance activities against Catalan activists in Switzerland,[21] as well as against members from the Scottish National Party after they had participated in a protest supporting the political prisoners in Catalonia.[22]

These examples, along with those revealed through the Pegasus revelations, establish now an urgent need to inspect and scrutinize Spain's current monitoring and surveillance practices, particularly as it relates to efforts to silence and disable dissenting opinions and civil society groups.

Conclusion & Recommendations

The Pegasus revelations, along with established patterns of systemic repression and judicial harassment of Catalan activists, epitomizes Spain's increasingly overt criminalisation of the country's peaceful and democratic movements which express their support for Catalonian self-determination. The reaction of the Spanish state to this expression of the legitimate aspirations of the Catalan society has been and continues to be entirely disproportionate, threatening the exercise of freedoms of expression, association and assembly, not only for the leaders of civil society and political groups, but for the Catalan people as a whole.

The ANC and UNPO are deeply concerned about the increasing use of surveillance technology by governments around the world to target, intimidate and retaliate against human rights defenders, and in particular, movements advocating for their right to self-determination. In particularly, we wish to raise significant concern over the increasingly shrinking space for civil society and human rights defenders around the world in light of the unchecked use of surveillance technologies, such as NSO Group's Pegasus technology.

The ANC and UNPO affirm that while private companies creating and distributing such technology must not enjoy impunity from the negative human rights impacts of their products and services, governments too must be held accountable. The Spanish State's use of espionage against Catalan civil society actors represents yet another unacceptable development in its persecution of the Catalan people.

---

[19]Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto, and Sarah McKune, "Pay No Attention to the Server Behind the Proxy Mapping FinFisher's Continuing Proliferation" *Citizen Lab,* 15 October 2015. Available at: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

[20]Benas Gerdziunas, "Belgium to investigate Spain's alleged spying on Puigdemont" *Politico,* 13 June 2018. Available at: https://www.politico.eu/article/investigation-spanish-secret-services-belgium-carles-puigdemont/.

[21]Newsbeezer, "Spain Spies on Catalans in Switzerland", *Newsbeezer*, 11 August 2019. Available at: https://newsbeezer.com/switzerlandeng/spain-spies-on-catalans-in-switzerland/.

[22]Greg Russel, "REVEALED: Scottish MPs have been watched by Spanish spies" *The National,* 11 July 2019. Available at: https://www.thenational.scot/news/17762296.revealed-scottish-mps-watched-spanish-spies/.

The ANC and UNPO call on the United Nations and wider international community to defend the fundamental rights of citizens around the world by holding country's accountable where satisfactory evidence of their unwarranted deployment of NSO Group's Pegasus can be attributed.

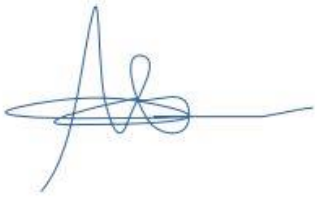
In light of credible reports that the Kingdom of Spain have used Pegasus spyware to unlawfully and arbitrarily monitor Catalan civil society, we request the following actions, or any combination of them, be taken by the Special Rapporteurs:

A) Issue a joint public statement (i.e the respective mandates) calling on Spanish authorities to cease these illegal practices against the victims.
B) Issue a Joint Allegation Letter to the Government of Spain on its alleged use of NSO Group's Pegasus technology to monitor Catalonian civil society. Specifically, where possible urging the Government of Spain to:
    I. Conduct an immediate, independent, transparent, impartial and effective investigation to identify and sanction those responsible for these facts;
    II. Provide detailed information on the purchase of spyware, including Pegasus, developed by NSO Group, and its alleged use targeting political opponents;
    III. Put an immediate end to this illegal practice, including the termination of any contract currently in force with the NSO Group or any company acting as an intermediary in the sale of the spyware;
    IV. Ensure reparation to victims, in particular by the communication of a complete report informing them on which data and conversations were obtained by the exploitation of the Pegasus software, which treatment was made of these data, and which persons and authorities were involved;
    V. Reform existing laws that pose barriers to remedy for victims of unlawful surveillance and implement domestic legislation that imposes safeguards against human rights violations and abuses through digital surveillance and establishes accountability mechanisms designed to provide victims of surveillance abuses of pathway to remedy;
    VI. Cease all acts of judicial harassment in connection to supporters of Catalonian independence;
C) Send a request for a country visit by the Special Rapporteurs addressed in this submission to assess the situation facing Catalonian civil society in light of the Government of Spain's alleged use of NSO Group's Pegasus technology;
D) Undertake visits (or other similar actions) in order to meet with impacted victims and to provide technical support to Spain in implement best practices regarding digital rights and lawful surveillance practices.
E) Undertake any other actions, as considered most appropriate, in order to secure the victims' rights, and others that may face or are facing a similar situation.

We would like to thank you for the attention you bring to the case and we remain at your disposal for any further information.

Sincerely,

Elisenda Paluzie
President, Catalan National Assembly



Mercè Monje Cano
Executive Director, UNPO