Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

PEGASUS and NSO Group cellular spying

Document published at www.cita.es/pegasus.pdf

From Madrid, Spain, **Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA**, is expert witnessing for Courts of Law on Pegasus, a spyware for governments improving commercial products like **FLEXISPY Mobile Spy Spy Phone** that can be installed on devices running some versions of iOS, Apple's mobile operating system, as well on devices running Android. It was developed by the Israeli cyberarms firm, NSO Group. Secret services are very aware of this kind of spyware risks and illegal advantages for Government surveillance activities. If no judge explicitly allow previously each time it is used for a forensic purpose there is serious criminal case no matter who and how used it.

APEDANICA is looking for documented cases of PEGASUS, **FLEXISPY Mobile Spy Spy Phone** as well as **CELLEBRITE** systems. For instance, **Catalan parliamentary speaker's cellphone was targeted with PEGASUS**. Citizen Lab states that **130 activists have been unjustified victims of the NSO program since 2016**. A messaging app account belonging to the Crown Prince of Saudi, Mohammed bin Salman, was used to deploy digital **spyware on the phone of Jeff Bezos, who is also CEO of Amazon**, "in an effort to influence, if not silence" the newspaper's reporting on the Kingdom.

APEDANICA is very pleased to receive and impart information regarding spyware with special attention to already spied victims following Universal Declaration of Human Rights article 19 "*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers*". We include anything not legally forbidden to be published related with agencies like:
National Security Agency NSA Главное Разведывательное Управление in Russian Federation State Security Service General Intelligence and Security Service, military intelligence ADIV/SGRS Coordination Unit for the Threat Assessment OCAD/OCAM in Belgium Nachrichtendienst des Bundes NDB in Switzerland Ministry of State Security MSS in China Reconnaissance General Bureau in North Korea Directorate of Military Intelligence DRM in France Algemene Inlichtingen- en Veiligheidsdienst AIVD in The Netherlands Bundesnachrichtendienst BND in Germany Εθνική Υπηρεσία Πληροφοριών ΕΥΠ in Greece Greiningardeild Varnarmálastofnunar Íslands GVMSÍ in Iceland Directorate General of GST Intelligence DGGI in India Ministry of Intelligence VAJA in Iran Inter-Services Intelligence ISI in Pakistan General Intelligence Presidency (GIP) – رئاسة الاستخبارات العامة in Saudi Arabia Federal Security Service FSB Федеральная служба безопасности and Main Intelligence Directorate GRU or Centro Nacional de Inteligencia CNI in Spain

RELEVANT REFERENCES FOR **APEDANICA** APPROACH

https://news.un.org/en/story/2020/01/1055771
Independent UN rights experts call for ‘immediate investigation’ into alleged Bezos phone hack by Saudi Arabia David Kaye (left), Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and Agnes Callamard, Special Rapporteur on extrajudicial, summary or arbitrary executions.UN Photo/Rick Bajornas/Loey Filipe David Kaye (left), Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression and Agnes Callamard, Special Rapporteur on extrajudicial, summary or arbitrary executions. 22 January 2020 Human Rights Independent UN rights experts said on Wednesday they were “gravely concerned” over allegations that in 2018, a messaging app account belonging to the Crown Prince of Saudi Arabia was used to hack into The Washington Post owner’s mobile phone, calling for an “immediate investigation” by authorities in the United States. The two Special Rapporteurs - who do not speak on behalf of the UN overall, and operate in an independent investigative capacity - said in a statement that they had recently received information suggesting that a WhatsApp account belonging to Crown Prince Mohammed bin Salman was used to deploy digital spyware on the phone of Jeff Bezos, who is also CEO of Amazon, “in an effort to influence, if not silence” the newspaper’s reporting on the Kingdom. “The allegations reinforce other reporting pointing to a pattern of targeted surveillance of perceived opponents and those of broader strategic importance to the Saudi authorities, including nationals and non-nationals”, said Agnes Callamard, UN Special Rapporteur on summary executions and extrajudicial killings, and David Kaye, UN Special Rapporteur on freedom of expression. “These allegations are relevant as well to ongoing evaluation of claims about the Crown Prince’s involvement in the 2018 murder of Saudi and Washington Post journalist, Jamal Khashoggi”. They spelled out that the alleged hacking of Mr. Bezos’ phone, and those of others, if proven, would be in contravention of fundamental international human rights standards, and demands an “immediate investigation” by US and other relevant authorities, “including investigation of the continuous, multi-year, direct and personal involvement of the Crown Prince in efforts to target perceived opponents”. Better controls needed The reported surveillance of Mr. Bezos, allegedly through software developed and marketed by a private company was “transferred to a Government without judicial control of its use”, said the experts. If true, they maintained it was “a concrete example of the harms that result from the unconstrained

marketing, sale and use of spyware". To protect against its abuse, surveillance through digital means must be "subjected to the most rigorous control", according to the independent experts, including by judicial authorities and national and international export controls. Moreover, they argued that "it underscores the pressing need for a moratorium on the global sale and transfer of private surveillance technology". "The circumstances and timing of the hacking and surveillance of Bezos also strengthen support for further investigation by US and other relevant authorities of the allegations that the Crown Prince ordered, incited, or, at a minimum, was aware of planning for but failed to stop the mission that fatally targeted Mr. Khashoggi in Istanbul", the UN experts stated. 'Clandestine' online campaign While the Kingdom was supposed to be investigating Mr. Khashoggi's murder and prosecuting those responsible, the Rapporteurs said, "it was clandestinely waging a massive online campaign against Mr. Bezos." A 2019 forensic analysis of his iPhone assessed with "medium to high confidence", that it was infiltrated on 1 May 2018 through a video sent from Mohammed bin Salman's WhatsApp account. According to the analysis, the Crown Prince and Mr. Bezos exchanged numbers the month before the alleged hack. The forensic analysis found that within hours of receiving the video from the Crown Prince's account, "an unprecedented exfiltration of data" from the iPhone began. After an initial spike, the unauthorized transfer of data continued undetected for months. The information we have received suggests...an effort to influence, if not silence, The Washington Post's reporting on Saudi Arabia -- UN Experts The analysis also assessed that the intrusion was likely undertaken through a prominent spyware that was identified in other Saudi surveillance cases, the experts said. They added that the allegations were reinforced by separate evidence of Saudi Arabia targeting dissidents and perceived opponents. The Saudi Arabian Embassy in Washington, said on Tuesday night that any suggestion the Kingdom was behind the hacking of Mr. Bezos' phone, "are absurd". Other reported cases The Special Rapporteurs noted that the claims regarding Mr. Bezos' hacked phone are also consistent with the widely reported role of the Crown Prince in allegedly leading a campaign against dissidents and political opponents. They recalled that the iPhone infiltration occurred from May to June in 2018, when the phones of Jamal Khashoggi's associates, Yahya Assiri and Omar Abdulaziz, were also hacked, allegedly using malware called Pegasus. In May 2018, Jamal Khashoggi was a prominent columnist for The Washington Post, writing stories that raised concerns about the Crown Prince's rule. That October, government officials murdered him in the Saudi consulate

in Istanbul, Turkey. The newspaper subsequently began covering extensively the disappearance and murder investigation and expanded its reporting on a number of related aspects of the Crown Prince's rule in Saudi Arabia. Breaking it down According to the forensic analysis, after Mr. Bezos' mobile was hacked, the Crown Prince sent him WhatsApp messages in November 2018 and February 2019, "in which he allegedly revealed private and confidential information about the billionaire publisher's personal life that was not available from public sources", said the experts. "During the same period, Mr. Bezos was widely targeted in Saudi social media as an alleged adversary of the Kingdom. This was part of a massive, clandestine online campaign against Mr. Bezos and Amazon, apparently targeting him principally as the owner of The Washington Post." Ms. Callamard and Mr. Kaye "expect to continue investigating the murder of Mr. Khashoggi and the growing role of surveillance in permitting the unaccountable use of spyware to intimidate journalists, human rights defenders and owners of media outlets", concluded the statement released by the UN human rights office, OHCHR. Independent experts' role Special Rapporteurs and independent experts are appointed by the Geneva-based UN Human Rights Council to examine and report back on a specific human rights theme or a country situation. The positions are honorary and the experts are not UN staff, nor are they paid for their work.

https://www.amnesty.org/en/latest/news/2020/07/israel-court-notorious-spyware-firm-nso/

ISRAEL AND OCCUPIED PALESTINIAN TERRITORIES HUMAN RIGHTS DEFENDERS AND ACTIVISTS SHARE Facebook Twitter Israel: Court rejects bid to revoke notorious spyware firm NSO Group's export licence 12 July 2020, 17:41 UTC Today's disgraceful ruling is a cruel blow to people put at risk around the world by NSO Group selling its products to notorious human rights abusers. Danna Ingleton, acting Co-Director of Amnesty Tech A Tel Aviv District Court today rejected an attempt, supported by Amnesty International, which sought to force Israel's Ministry of Defence (MOD) to revoke the security export license of spyware company NSO Group. Danna Ingleton, acting Co-Director of Amnesty Tech, said: "Today's disgraceful ruling is a cruel blow to people put at risk around the world by NSO Group selling its products to notorious human rights abusers. At a moment when NSO and the Israeli MOD should be held accountable for their practices, it is appalling that the court has failed to do so. "NSO Group continues to profit from human rights abuses with impunity. The ruling of the court flies in the face of the mountains of evidence of NSO Group's spyware being used

to target human rights defenders from Saudi Arabia to Mexico, including the basis of this case - the targeting of one of our own Amnesty employees. We will continue to do all we can to stop NSO Group's spyware being used to commit human rights abuses. "Until there is transparency around NSO's business practices and guarantees that the Israeli MoD process of granting export licenses is set according to international standards and practices, the company's products will continue to aid in the persecution of activists and the repression of human rights." Background The legal action - brought by members and supporters of Amnesty International Israel and others- comes after evidence has emerged showing how NSO spyware technologies, most notably Pegasus, have been used to target an Amnesty International employee as well as numerous journalists and activists, including in Morocco, Saudi Arabia, Mexico and the UAE. The legal case is supported by Amnesty as part of a joint project with New York University School of Law's Bernstein Institute for Human Rights and the Global Justice Clinic.

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
Catalan parliamentary speaker's cellphone was targeted with a spy program only available to governments A Canadian cybersecurity institute that investigated a fault in WhatsApp discovered that Roger Torrent's handset was attacked in 2019 together with a hundred other figures from civil society around the world Catalan parliamentary speaker Roger Torrent. Catalan parliamentary speaker Roger Torrent.TONI ALBIR / EFE JOAQUÍN GIL Madrid - 14 JUL 2020 - 09:30 CEST The cellphone used by the speaker in the Catalan regional parliament, Roger Torrent, was targeted with Pegasus, a spy program developed by an Israeli company named NSO, and which can only be purchased by governments and security forces and used to target crime and terrorism. Torrent's phone was attacked using Pegasus in 2019, according to a joint investigation by EL PAÍS and The Guardian. The intrusion into the handset of the pro-Catalan independence politician, who belongs to the Catalan Republican Left (ERC) party, was possible due to a security fault in the WhatsApp messaging service that, between April and May 2019, could be used to install the NSO spy program in at least 1,400 cellphones across the world. The method for the attack was a missed video call, according to WhatsApp. When you find a Pegasus target, you find the fingerprints of a government CITIZEN LAB RESEARCHER JOHN SCOTT-RAILTON Pegasus took advantage of this weakness to

attack Torrent's phone, according to Citizen Lab, a cybersecurity group from the Munk School of Global Affairs and Public Policy at the University of Toronto, which exclusively investigated the fault in the messaging application in 2019. WhatsApp supplied Citizen Lab with the numbers that had been targeted by the Israeli cyberespionage program, among which was that of Torrent, according to these researchers, who publicly revealed the existence of Pegasus. EL PAÍS and The Guardian have had access to a certificate emitted by Citizen Lab that validates the fact that the speaker's phone was attacked with the NSO spyware. "The investigation identified that the number belongs to Mr Roger Torrent," the analysis states. The document explains that the attackers resorted to a missed WhatsApp call "that did not require a response" to target the politician's phone, and it contains "ample evidence that could establish that Torrent was monitored." Torrent's phone figures on a list of a hundred or so cases across the world that were compiled by Citizen Lab of "representatives of civil society" who were indiscriminately attacked via the WhatsApp vulnerability, according to the Canadian institution. Citizen Lab states that 130 activists have been unjustified victims of the NSO program since 2016. Pegasus permits conversations to be listened to, messages read, access to the phone's memory, screenshots to be taken, browsing history to be tracked and for remote access of the device's microphone and camera. This opens the door for the program to listen to the ambient sound in a room if a phone has been infected. The system even allows for encrypted messages and voice calls to be recorded, according to the Canadian experts. In 2018, Pegasus was being used in 45 countries, targeting activists in Bahrain, Kazakhstan, Saudi Arabia, the United Arab Emirates and Mexico The researchers connected the mysterious disappearance of WhatsApp messages from Torrent's cellphone in 2019 with an indication that the phone "could have been manipulated by a third party and infected." And while they cannot identify who ordered the attack, they point out that the Israeli firm that created Pegasus "exclusively sells its products to governments." This fact is confirmed by NSO on its website, where it presents its services as solutions for the armed forces and the police to combat crime. While Torrent's cellphone was targeted by Pegasus, in 2019, the parliamentary speaker took part in dozens of political meetings and also appeared as a witness in Spain's Supreme Court during the trial of the politicians and civil leaders who were involved in the 2017 independence drive in the Catalonia region, which saw an illegal referendum on secession from Spain held in October of that year. Among the sentences handed down by the court, Carme Forcadell, Torrent's predecessor as speaker in the regional parliament, was given 11-and-a-half years in jail for the offense

of sedition. In May 2019, when he was being targeted with Pegasus, Torrent took part in a meeting in Strasbourg with the Council of Europe Commissioner for Human Rights, Dunja Mijatvic. “I noticed strange things,” Torrent explains. “WhatsApp messages and chat histories would be deleted. It didn’t happen to the people around me.” The politician also says that he received “strange” SMS messages in 2019. Torrent says that he sees the hand of the “Spanish state” behind the Pegasus attack. “The government has no evidence that the speaker of the Catalan parliament, Roger Torrent [...] [has] been the targets of hacking via their mobiles,” says a spokesperson from the Spanish government, who points out that any monitoring of communications requires a court order. A spokesperson from the CNI, Spain’s intelligence services, says that the organization acts “in full accordance with the legal system, and with absolute respect for the applicable laws.” The same spokesperson adds that the actions of the secret service are supervised by a magistrate from the Supreme Court. EL PAÍS and The Guardian have unsuccessfully tried to obtain the versions of the Civil Guard, the National Police and the Interior Ministry as to what happened. Citizen Lab recognizes the difficulty of proving the reach of the cyber attack on Torrent’s cellphone, given that, as it indicates, the NSO programs “have an erasing system on the devices.” “When you find a Pegasus target, you find the fingerprints of a government,” says the researcher from this group, John Scott-Railton. We can confirm that Torrent’s telephone was targeted. However, additional investigation would be necessary to confirm that the phone was hacked CITIZEN LAB RESEARCHER JOHN SCOTT-RAILTON According to the expert, “we can confirm that [Torrent’s] telephone was targeted. However, additional investigation would be necessary to confirm that the phone was hacked. At this time we have no reason to believe that it wasn’t.” After being informed about the issue by this newspaper, Torrent’s team got in touch last Thursday with Scott-Railton. “They gave us the cellphone of the parliamentary speaker without us having asked for it and they said that it was among those attacked by Pegasus,” a spokesperson for the politician explains. “Was the infection successful? [Citizen Lab researcher John] Scott-Railton believes so because Torrent’s WhatsApp messages in 2019 were erased, which is one of the effects of Pegasus.” Controlled by the London-based fund Novalpina Capital, NSO says that it has a policy for the investigation of the improper use of its systems. NSO has refused to clarify if Spain is among its clients. “Due to confidentiality agreements, we cannot confirm which authorities use our technology,” the company replied via email. The firm has said that it will begin an investigation “if it is proved” that its products were used improperly in

Spain. The Israeli company has distanced itself in the United States' courts from the improper use of its spy program. The firm attributes this responsibility to its clients, the governments who acquire its products. "If anyone installed Pegasus on any alleged 'target devices' it was not [the] defendants [NSO Group]. It would have been an agency of a sovereign government," the company stated as a defense in a lawsuit that it is involved in with WhatsApp. The messaging application reported NSO in October of last year for using its platform to infect the cellphones of activists and diplomats around the world with Pegasus. There is no evidence that Spain's security forces are clients of NSO. The National Police and the CNI did hire their main competitor, Hacking Team from Italy, until at least 2015. This emerged after 400 gigabytes of internal emails from this company were stolen from its servers after they themselves were hacked. In 2018, Pegasus was being used in 45 countries, according to Citizen Lab, targeting activists in Bahrain, Kazakhstan, Saudi Arabia, the United Arab Emirates and Mexico. The cellphones of 25 Mexican politicians, activists and reporters, including the journalists Carmen de Arístegui (Arístegui Noticias), Andrés Villareal and Ismael Bojórquez (Río Doce) and Carlos Loret de Mola (Televisa) were targeted in 2019. As were three members of the organization Mexicans Against Corruption and Impunity, while the leaders of the National Action Party (PAN) Ricardo Anaya and Fernando Rodríguez Noval were also monitored. Omar Radi, a 33-year-old Moroccan journalist, also saw his phone infected by Pegasus after he criticized a judge. OTHER VICTIMS OF PEGASUS As well as Catalan speaker Roger Torrent, Pegasus also targeted the cellphone of Anna Gabriel, a former deputy in the Catalan parliament for the anti-capitalist CUP party, and her lawyer, Olivier Peter. Gabriel fled Spain in 2018 and traveled to Switzerland to avoid testifying before Spanish Supreme Court Judge Pablo Llarena over allegations of rebellion, misappropriation of public funds and sedition in connection to her role in the 2017 Catalan breakaway bid. "[Gabriel] received a WhatsApp notification that told her that her cellphone could have been hacked," explained Peter, alluding to a vulnerability the messaging service suffered between April and May in 2019, which was later fixed. "If the hack is confirmed and we have more information, action will be taken," he added. Jordi Domingo, a staff member of the Tarragona provincial government, was another victim of Pegasus, according to the investigation from EL PAÍS and The Guardian. "That's right. The investigator from Citizen Lab, John Scott, called me last October to tell me that my cellphone was hacked before 2019," said Domingo, who is also a member of the Asamblea Nacional Catalana (ANC) and the separatist Catalan European Democratic Party

(PdeCAT). Domingo suggested two reasons for why he may have been targeted. “The first is that it was all a mistake. I have the same name as a well-known separatist lawyer. And the second [is] because I asked Barcelona city hall in 2018 for authorization on behalf of the Observatory against Catalanphobia to hold a demonstration. That very day, the police union Jusapol, held a march.” According to Domingo, he was not subject to any legal investigation during the time his cellphone was hacked by Pegasus. When asked if he would report the incident, he replied: “Who would I report? I don’t know who spied on me.” A spokesperson from the Spanish government said that there was “no evidence” that Gabriel and Domingo had been spied on. English version by Simon Hunter.

https://www.theguardian.com/world/2020/jul/14/second-catalan-politician-says-phone-was-targeted-by-spware

Second Catalan politician says phone was targeted by spyware Ernest Maragall revelation set to boost calls for inquiry into possible domestic espionage Stephanie Kirchgaessner, Sam Jones in Madrid and Jennifer Rankin in Brussels Tue 14 Jul 2020 19.02 BSTLast modified on Tue 14 Jul 2020 20.45 BST Shares 130 Ernest Maragall Ernest Maragall said researchers working with WhatsApp told him his phone was targeted in 2019. Photograph: Europa Press News/Getty Images A second prominent member of Catalan’s pro-independence movement has revealed he was warned that his mobile phone was targeted using spyware. The development is likely to bolster calls for an investigation into the possible use of hacking technology by Spanish authorities. Ernest Maragall, an MP in the regional parliament and a former member of the European parliament who also served as Catalan foreign minister, told the Guardian and El País that he was alerted by researchers working with WhatsApp that his phone had been targeted last year. A joint investigation by the newspapers revealed on Monday that Roger Torrent, the speaker of the Catalan parliament, was also targeted in 2019, according to researchers at Citizen Lab at the University of Toronto, who have collaborated with WhatsApp. Advertisement “It is terrible,” Maragall said. “This is not a surprise. It is just a part of the techniques, of the reality we are living in every day. We are in a situation where judicial actions, policies, security forces, prosecutors, everybody ... is against our movement, our peaceful and democratic movement as citizens here in Catalonia.” Torrent and Maragall – as well as two other pro-independence activists – were alerted that they were targeted in April-May 2019, when spyware used by government clients around the

world exploited a previous vulnerability in WhatsApp software. The spyware, made by Israel's NSO Group, allows the operator of the hacking tool to access an individual's phone, including emails, calls and text messages. NSO Group has said it has no knowledge or control over how its clients use the spyware. Current and former leaders of Catalonia's pro-independence government have called for an inquiry into what one researcher at Citizen Lab called a "possible case of domestic political espionage" in Europe. Torrent called the reports "extraordinarily serious", adding: "We cannot normalise spying on political dissidence." He said that if the Spanish government knew of the facts in the case "then it would have been complicit in a crime". If it did not, he said, "it would be a very worrying symptom of political negligence and unawareness of illegal practices". Gabriel Rufián, the spokesman in the national parliament for the Catalan Republican Left party, called on Spain's interior minister, Fernando Grande-Marlaska, to "provide explanations over the alleged spying and invasion of privacy against Catalan political leaders by government organisations". The revelations also resonated in the European parliament, where one of the most senior allies of Pedro Sánchez, the Spanish prime minister, called for an investigation into the targeting of Torrent's phone. Juan Fernando López Aguilar, a Spanish Socialist MEP who chairs the European parliament's civil liberties committee said: "Any indication that there might have been an intrusion in the confidentiality of data of European citizens – be it high officials, representatives, or private citizens for that matter – should be thoroughly investigated." In Spain, he said, such investigations are a matter for the public prosecutor. He added that there was "no ground whatsoever to point out the responsibility of any national agency or government [in connection] to that information we have just read of". The Spanish government said it was a legal, rather than political matter, and suggested that Torrent report his concerns to the judicial authorities. "The government has no evidence that the speaker of the Catalan parliament has been the victim of a hack or theft involving his mobile," the government's spokeswoman, María Jesús Montero, told reporters on Tuesday afternoon. "When questions of this nature arise, the procedure is well known: you inform the relevant judicial authorities about the hack or tapping, or the theft from a device, and they can then investigate whether it has happened and under what circumstances. Any mobile phone tapping always requires preliminary judicial authorisation. This isn't something for the government." In a statement, Spain's interior ministry said: "Neither the interior ministry, nor the national police, nor the Guardia Civil have ever had any relationship with the company that developed this program, and, as such, have never contracted its

services." It added that the actions of state security forces were always conducted "with the utmost respect for the law". Spain's National Intelligence Centre (CNI) said in a statement that it acted "in full accordance with the legal system, and with absolute respect for the applicable laws" and that its work was overseen by Spain's supreme court. It did not respond to specific questions about the alleged use of "Pegasus" spyware sold by NSO Group. WhatsApp has said that a total of 1,400 users were targeted in the 2019 attack, which is now the subject of a lawsuit by the messaging app against NSO Group. The California company has claimed that 100 members of civil society – including journalists in India, human rights activists in Morocco, diplomats and senior government officials – are alleged to have been affected. NSO Group has denied it has any role in operating its hacking software and has said it has no knowledge of who its government clients target. The company said it operated under "industry-leading governance policies" and that it could not confirm or deny which authorities used its technology because of confidentiality constraints. The company has been critical of Citizen Lab, which has closely researched the use of NSO Group's spyware, and said researchers had failed to "competently address the challenges faced by law enforcement agencies" who need to intercept encrypted communications. NSO Group has said it sells its spyware solely for governments to track terrorists and criminals. López Aguilar, who worked on the European parliament's response to 2013 revelations that the US National Security Agency had hacked the telephone records of millions of people, said all EU member states were bound to follow European law on data privacy, including the General Data Protection Regulation. "Any member states that might have some breach of that European law should be accountable for it, but those reports first of all have to be fully verified. Protection of rights and privacy are of the essence for the consistency of Europe."

https://www.theguardian.com/world/2020/apr/07/nso-group-points-finger-at-state-clients-in-whatsapp-spying-case

NSO Group points finger at state clients in WhatsApp spying case This article is more than 3 months old In court filing, Israeli spyware company says it does not operate technology it provides Stephanie Kirchgaessner in Washington @skirchy Email Tue 7 Apr 2020 18.13 BSTLast modified on Tue 7 Apr 2020 22.14 BST Shares 73 The offices of NSO group, in Herzliya, near Tel Aviv. WhatsApp has accused the company of hacking 1,400 of its users The offices of NSO group, in Herzliya, near Tel Aviv. WhatsApp has accused the company of hacking

1,400 of its users. Photograph: Jack Guez/AFP via Getty Images An Israeli spyware company that has been accused by WhatsApp of hacking 1,400 of its users, including journalists, human rights activists, and diplomatic officials, has blamed its government clients for the alleged abuses, according to court documents. NSO Group – whose technology is reported to have been used against dozens of targets including Pakistani intelligence officials, Indian journalists and exiled Rwandan political activists – also claimed in legal documents that the lawsuit brought against the company by WhatsApp threatened to infringe on its clients' "national security and foreign policy concerns". WhatsApp sues Israeli firm, accusing it of hacking activists' phones Read more NSO Group has never disclosed a full list of its government clients, but research by Citizen Lab, which tracks the use of spyware, has claimed that current and former clients include Saudi Arabia, Bahrain, Kazakhstan, Morocco, Mexico and the United Arab Emirates. WhatsApp, the popular messaging app, filed a lawsuit against NSO Group in October, alleging that the cyberweapons company was behind a series of highly sophisticated attacks that it claimed violated US law in an "unmistakeable pattern of abuse". Among the alleged victims of the hack, which was discovered last April and continued for two weeks until the app's vulnerability was fixed, were 100 human rights activists, lawyers, journalists and academics who were later notified of the alleged intrusion by WhatsApp. Advertisement In its first substantive legal filing in the case, filed last week, NSO hit back at WhatsApp and its parent company, Facebook, which it said were seen by governments as "safe spaces for terrorists and other criminals" who – without NSO's services – could operate "without fear of detection by law enforcement". NSO Group also argued that WhatsApp had "conflated" NSO Group's actions with the actions of NSO's "sovereign customers". While NSO Group licenses its signature spying technology, Pegasus, to government law enforcement and intelligence agencies and assists with "training, setup, and installation", it said it did not operate the technology. "Government customers do that, making all decisions about how to use the technology," NSO said in its legal filing. "If anyone installed Pegasus on any alleged "target devices" it was not [the] defendants [NSO Group]. It would have been an agency of a sovereign government." NSO Group claimed that to challenge such conduct, WhatsApp would have to declare the "sovereign acts" of those governments to be illegal. "For that reason," the company said in the filing, "permitting this litigation to proceed would infringe critical national security and foreign policy concerns of sovereign governments". The company also highlighted the role it claimed the Israeli government played in its review of NSO

Group's business. The Israeli ministry of defence, NSO Group said, could have access to information about NSO Group's customers and "their intended use of Pegasus technology". In a statement, WhatsApp said NSO Group was attempting to "avoid responsibility" and questioned the accuracy of some of the company's claims, including an allegation in the legal filing that Facebook had wanted to procure some of NSO Group's technology in 2017. In a sworn statement filed to the court, Shalev Hulio, an NSO Group co-founder, said that NSO had been approached by two Facebook representatives in October 2017 and asked about the right to "certain capabilities of Pegasus", which the representatives had suggested could be used to help monitor users on Apple devices. NSO Group declined to comment to the Guardian's questions about the alleged meeting between Facebook and NSO, and said it would not reveal the identity of the individuals. WhatsApp said the description of the discussions were an "inaccurate representation". It declined to provide further comment.

HIDE AND SEEK: Tracking **NSO** Group's **Pegasus** Spyware to operations in 45 countries

B Marczak, J Scott-Railton, S McKune, B Abdul Razzak… - 2018 - tspace.library.utoronto.ca

Licensed under the Creative Commons BY-SA 4.0 (Attribution-ShareAlike licence). Electronic version first published in 2018 by the Citizen Lab … This work can be accessed through https://citizenlab.ca/2018/09/hide- and-seek-tracking-**nso**-groups-**pegasus**-spyware-to-operations …

The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power: Shoshana Zuboff. 2019, New York: Public Affairs.

J Sarah Sam - 2020 - Taylor & Francis

… "HIDE AND SEEK: Tracking **NSO** Group's **Pegasus** Spyware to operations in 45 countries." https://citizenlab.ca/2018/09/hide-and-seek-tracking-**nso**-groups-**pegasus**-spyware-to-operations-in-45-countries/

Reckless VI: Mexican Journalists Investigating Cartels Targeted with **NSO** Spyware Following Assassination of Colleague

J Scott-Railton, B Marczak, S Anstis, BA Razzak… - 2018 - tspace.library.utoronto.ca

… Table 1. **NSO** Group **Pegasus** Exploit Domains Used in this Operation Page 11. 11 … In September 2018, prior to the publication of another Citizen Lab report on **NSO** Group's **Pegasus** spyware, **NSO** Group reiterated that it "develops products …

Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel

E Zureik - Middle East Critique, 2020 - Taylor & Francis

… individual privacy. However, after extensive investigation into the **NSO's** mode of operation in Mexico, a report concluded there was no evidence that the use of **Pegasus** and other **NSO** products resulted in positive outcomes.

Some references of **APEDANICA**

Palestinian BDS National Committee BNC

Document published at www.cita.es/anyvision-palestinians.pdf

From Madrid, Spain, **Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas** **APEDANICA**, is investigating AnyVision Israel based company and we have seen published this AnyVision | BDS Movement

Boycott AnyVision: Israel's "field-tested" facial recognition surveillance company

The Palestinian BDS National Committee (BNC) calls for boycotting AnyVision, Israel's facial recognition technology firm, due to its irrefutable complicity in Israel's occupation and repression of Palestinians.

August 30, 2019 By: Palestinian BDS National Committee (BNC)

Considering complaints filled by **APEDANICA**, Spanish privacy authority AEPD investigates AnyVision business and technologies for Mercadona. We shall appreciate any relevant information useful not only for Spain, but also for the European Union. We suggest to read next document www.europarl.europa.eu/doceo/document/O-9-2020-000018_EN.html

Parliamentary questions O-000018/2020 Question for oral answer to the Commission Rule 136 Manon Aubry, Anne-Sophie Pelletier, Philippe Lamberts, Manuel Bompard, Leila Chaibi, Clara Ponsatí Obiols, Mick Wallace, Idoia Villanueva Ruiz, Konstantinos Arvanitis, Cornelia Ernst, Emmanuel Maurel, David Cormand, Younous Omarjee, Alexandra Geese, Saskia Bricmont, Viktor Uspaskich, Patrick Breyer, Rosa D'Amato, Markéta Gregorová, Aurore Lalucq, Helmut Scholz, Isabella Adinolfi, Marie Toussaint, Henrike Hahn, Martina Michels, Niyazi Kizilyürek, Fabio Massimo Castaldo, Hilde Vautmans, Pierre Larrouturou, Yannick Jadot, Raphaël Glucksmann, Paul Tang, Nora Mebarek, Stelios Kouloglou, Miguel Urbán Crespo, Alexis Georgoulis, Malin Björk, Petra De Sutter, Ernest Urtasun, Anna Cavazzini, Özlem Demirel, Petros Kokkalis, José Gusmão, Marc Botenga, Maite Pagazaurtundúa, Eugenia Rodríguez Palop, Marisa Matias, Helmut Geuking, Benoît Biteau, Gwendoline Delbos-Corfield, Claude Gruffat, Michèle Rivasi, Caroline Roose Subject: Facial recognition and identification in publicly accessible spaces 1. In the context of the preparation of the White Paper on Artificial Intelligence and the Strategy for Europe – Fit for the Digital Age, does the Commission consider the deployment of facial recognition and/or facial identification systems in publicly accessible spaces by Member States to be inconsistent with Article 9(1) and 9(2)(g) of the General Data Protection Regulation (GDPR) – since it does not meet the requirement of being 'necessary for reasons of substantial public interest' – and Articles 4(1), 8(1) and 10 of the Law Enforcement Directive? 2. Does the Commission identify risks of violations of fundamental rights posed by the deployment of facial recognition and/or facial identification systems in publicly accessible spaces by Member States? 3. If so, is the Commission, as guardian of the treaties, considering banning such practices and/or launching infringement procedures against Member States? Submitted: 01/03/2020

APEDANICA shall be pleased to cooperate with anybody interested in that European Parliamentary question and the next 9 pages in Spanish.

Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

Nancy Pelosi Speaker of the House of Representatives

Open letter published at www.cita.es/nancy-pelosi-donald-trump.pdf

Dear Madam, **Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA** from Madrid, Spain, is concerned regarding evidences on **CORONAVIRUS COVID-19 pandemic** responsibility at the **World Health Organisation WHO** as well as the United States Intelligence best sources. "***President Donald J. Trump*** *Is Demanding Accountability From the World Health Organization*" as we can read at https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-demanding-accountability-world-health-organization/ something widely approved by Europe and Spanish speaking countries.

However, we would like to ask for the same accountability from all public organisations and officials working in any country, including intelligence services of US (**Central Intelligence Agency CIA**) and Spain (**Centro Nacional de Inteligencia CNI**), serving in China, or in Italy. Future serious investigations of public responsibility will require most relevant data and metadata, now in computers and international communications in order to evidence who firstly knew what was done with epidemiology sensitive information. Intelligence must be useful for Health authorities, but not for illegal business opportunities, from officials to speculators.

In Spain and Spanish speaking countries **APEDANICA** has already recommended to preserve every shred of evidence and documents from public servers in China and Italy, as well as stock market records. We suggest to focus Justice and political attention on data or metadata from US Embassy in China to White House since 2019 until current date.

Any official source in China can be relevant for the best intelligence on what was occuring, who knew it, and what was done with data and metadata sensitive information before and after the pandemic was declared by World Health Organisation WHO. Very few authorities can access the computer documents, emails and smartphones data and metadata. We will be obliged if the **US Speaker of the House of Representatives** could find the best procedure to obtain and preserve the evidence that President Donald Trump supposedly knew, and when he was aware of the real pandemic risk, as well as any illegal business profit made from privileged information, including any stock market illegal speculation. With a view to assist with enquiries we attach **40 pages in this PDF, asking for your acknowledgement of receipt soon.**

Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf

Attorney General Freedom of Information Act FOIA

published at www.cita.es/coronavirus-attorney-general.pdf

Spanish non-for-profit **Asociación para la Prevención y Estudio de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas APEDANICA** (founded in 1992) asks for information on any plaintiff or relevant data or references for expert witnessing and forensic purposes. For instance, right now we are looking for documents about **CORONAVIRUS COVID-19 related plaintiffs, in any country or any language**, as well as any record, in any Attorney General official files, that can be useful in any Court of Law. We have read this: "***On my watch, we will not tolerate schemes or frauds designed to turn large profits by exploiting people's health concerns***" said New York Attorney General James at https://www.blackstarnews.com/ny-watch/news/new-york-attorney-general-james-price-gouging-during-coronavirus-crisis

Moreover, **APEDANICA** is seriously concerned about massive data espionage by companies, like Google (Alphabet), and what have been published about ***"Project Nightingale"*** or with the Federal inquiry at https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867

So, considering **Freedom of Information Act 1982 (FOI Act)** and any other US Law useful for our request to the Attorney General, we ask for:

1º Any record in any file related with **CORONAVIRUS COVID-19**

2º Any record related with **Google and Health** data protection and risks, as well as any technology big company with access to Health metadata like ***"Project Nightingale"***, if the attorney general is already aware of.

3º Any record that could be related with ***schemes or frauds designed to turn large profits by exploiting people´s health concerns***

APEDANICA shall be pleased to be useful for any official or investigator and we shall do our best to share our concerns and relevant information with experts from all over the World. In order to explain our approach to **CORONAVIRUS COVID-19** and ***"Project Nightingale"*** we attach some documents already known by **World Health Organization WHO** representatives and epidemiology experts in several countries, while we work by **WhatsApp Groups** with many people that share our interest and Philosophy beyond our official records and files request. Please help us to be useful and do not hesitate to contact me to help you to find the records, because we are sure that attorneys and judges need them too.

Google Sued in Spain Over Data Collecting - The New York ...
www.nytimes.com › technology
18 ago. 2010 - “We are dedicating a lot of our time to finding a solution so that users ... Spanish association of Internet users, whose acronym is Apedanica, …

Spain investigates Google Street View wi-fi snooping - BBC.com

www.bbc.com › news › technology...

17 ago. 2010 - It is in response to a **complaint** by a privacy watchdog called **Apedanica**. The Google representative has been summoned to explain what data ...

Investigations of Google Street View - EPIC

epic.org › privacy › streetview

Unknown: **Street View** cars have gathered data from at least some locations, but ... as Internet **Giant** Calls Incidents "Accident", Gabriella Hold, Prague Post, May 26, ... In the **complaint**, **APEDANICA president Miguel Gallardo rejects Google's** …

[PDF] Запровадження міжнародних правових засада та іноземного досвіду у діяльності атикорупційної прокуратури
ЄВ Вандін - Право. ua, 2016 - irbis-nbuv.gov.ua
… 10. Asociación para la Prevención y Estudios de Delitos, Abusos y Negligencias en Informática y Comunicaciones Avanzadas (**APEDANICA**) [Електронний ресурс].– Ре- жим доступу: http://www.cita.es/**apedanica**/ 11. United …

Dr. (PhD) Miguel Á. Gallardo, Tel. +34 902998352

www.cita.es › fcc-complaint

APEDANICA now ask for FCC attention to some very dangerous and maybe criminal ... Hiperenlaces en www.cita.es/flexispy y www.miguelgallardo.es/flexispy.pdf ... kind of espionage under Freedom of Information Act (FOIA) as soon as possible. This complaint can be forwarded to any authority in any country and we keep ...

FEDERAL COMMUNICATIONS COMMISSION FCC - CITA

19 nov. 2018 - **Complaint** against Twitter Inc. SPOOFING in English and Spanish ... **APEDANICA** asks to FCC, under FOIA , any and all information about.

PEGASUS and NSO Group cellular spying

Document published at www.cita.es/pegasus.pdf

Dr. (PhD) Miguel Gallardo PERITO Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com
Asociación APEDANICA con registro del Ministerio del Interior www.cita.es/apedanica.pdf