DIARI DE SESSIONS
DEL PARLAMENT DE CATALUNYA

XIV* legislatura · cinquè període · sèrie C · número 600

Comissió d'Investigació sobre l'Espionatge de Representants Polítics, Activistes, Periodistes i llurs Familiars per part del Regne d'Espanya amb els Programes Pegasus i Candiru

Sessió 6, divendres 31 de març de 2023

Presidència de l'Il. Sr. Josep M. Jové Lladó

TAULA DE CONTINGUT

Compareixença de José Navarro, perit informàtic
357-00997/13 4

Compareixença d'Elies Campo, membre de The Citizen Lab, en qualitat de testimoni
365-00010/13 27

* Denominació que adopta la legislatura actual a partir del 4 de juny de 2021, en compliment de la Resolució 9/XIII del Parlament de Catalunya, aprovada pel Ple en la sessió 7, del 2 de juny de 2021 (BOPC 50/13, del 04.06.2021).

Aquesta publicació és impresa en paper ecològic (definició europea ECF), en compliment del que estableix la Resolució 124/III del Parlament, sobre la utilització del paper reciclat en el Parlament i en els departaments de la Generalitat, adoptada el 30 d'abril de 1990.

El *Diari de Sessions del Parlament de Catalunya* (DSPC) reprodueix només les intervencions orals fetes durant la sessió. La resta de documentació que acompanya la intervenció es pot consultar a l'expedient de la comissió.

Transcripció i correcció: CPSL
Imprès al Parlament

ISSN: 0213-7976 (general)
0213-7992 (sèrie C)
DL: B-3.468-1982

www.parlament.cat

Sessió 6 de la CIERPAPFRE

La sessió de la Comissió d'Investigació sobre l'Espionatge de Representants Polítics, Activistes, Periodistes i llurs Familiars per part del Regne d'Espanya amb els Programes Pegasus i Candiru (CIERPAPFRE) s'obre a les deu del matí i cinc minuts. Presideix Josep M. Jové Lladó, acompanyat del vicepresident en funcions Josep Jubert Montaperto i del secretari en funcions Xavier Pellicer Pareja. Assisteix la Mesa la lletrada Esther Andreu i Fornós.

Hi són presents Oscar Aparicio Pedrosa, pel G. P. Socialistes i Units per Avançar; Jordi Orobitg i Solé, pel G. P. d'Esquerra Republicana; Joaquim Jubert Montaperto i Josep Rius i Alcaraz, pel G. P. de Junts per Catalunya; Montserrat Vinyets Pagès, pel G. P. de la Candidatura d'Unitat Popular - Un Nou Cicle per Guanyar; Jessica González Herrera, pel G. P. d'En Comú Podem, i Ignacio Martín Blanco, pel G. P. de Ciutadans.

Assisteixen a aquesta sessió el perit informàtic José Navarro Hernández i el membre de The Citizen Lab Elies Campo.

ORDRE DEL DIA DE LA CONVOCATÒRIA

Punt únic: compareixença de José Navarro, perit informàtic, davant la Comissió d'Investigació sobre l'Espionatge de Representants Polítics, Activistes, Periodistes i llurs Familiars per part del Regne d'Espanya amb els Programes Pegasus i Candiru (tram. 357-00997/13). Comissió d'Investigació sobre l'Espionatge de Representants Polítics, Activistes, Periodistes i llurs Familiars per part del Regne d'Espanya amb els Programes Pegasus i Candiru. Compareixença.

El president

Molt bé, doncs, molt bon dia i gràcies per la seva assistència en aquesta sessió de la Comissió d'Investigació sobre l'Espionatge de Representants Polítics, Activistes, Periodistes i llurs Familiars per part del Regne d'Espanya amb els programes Pegasus i Candiru.

Tenim un ordre del dia inicialment d'un punt, que era la compareixença del senyor José Navarro com a pèrit informàtic. I també hi havia la possibilitat de que hi hagués la compareixença del senyor Elies Campo, membre de Citizen Lab, que compareixia com a testimoni i vam fer la convocatòria i saben que pel Reglament els testimonis tenen quinze dies de garantia per poder-se personar, venir i comparèixer a les comissions. Però li vam comentar que teníem aquesta comissió convocada, que si ell renunciava aquests quinze dies de termini i venia abans, podia fer-ho; i ens ha contestat que sí, i el tenim aquí. Per tant, podríem fer aquestes dues compareixences, d'acord?

També donem la benvinguda al representant de Ciutadans, que ahir ens van fer saber que participarien de la comissió i el senyor Nacho Martín Blanco, doncs, el tenim aquí. Moltes gràcies per la seva assistència i esperem comptar amb la seva participació per esclarir tots aquests fets. Sense res més, anirem a buscar el primer compareixent, senyor José Navarro, i faríem la seva compareixença.

Jessica González Herrera

President, aprofito per anunciar la substitució. *(Veus de fons.)* Sí, sí, sí.

El president

Sí, perdoni.

Jessica González Herrera

Només aprofito per anunciar la substitució del diputat Lucas Ferro, del Grup Parlamentari En Comú Podem, per mi mateixa.

El president

Molt bé, moltes gràcies. Alguna altra substitució?

Jordi Orobitg i Solé

President, en el mateix sentit, jo mateix substituiré la nostra portaveu en aquesta comissió, la diputada Marta Vilalta.

El president

Molts gràcies. *(Josep Rius i Alcaraz demana per parlar.)* Senyor Rius...

Josep Rius i Alcaraz

El senyor Jové, el senyor Batet.

El president

És veritat.
(Pausa.)

Compareixença de José Navarro, perit informàtic

357-00997/13

Doncs molt bé. Ja tenim el compareixent, el senyor José Navarro, pèrit informàtic. Li agraïm molt la seva presència avui aquí en aquesta sessió de la comissió d'investigació. Com saben, el que farem serà primer donar-li la paraula a vostè amb un temps aproximat..., posarem un temps màxim. Allà té el cronòmetre, de trenta minuts. Esgoti si ho considera oportú aquest temps, si no el temps que vostè consideri oportú. Després donaríem la paraula a tots els grups parlamentaris, als portaveus dels grups parlamentaris, per un temps de cinc minuts per a cada grup parlamentari. Quan acabin de fer les preguntes o els aclariments que necessitin els grups parlamentaris, li tornem a donar la paraula a vostè per deu minuts i contesta aquestes preguntes o aquests comentaris. Evidentment, serem flexibles amb el temps i si necessitem més temps, doncs, ho faríem així, d'acord?

Moltíssimes gràcies. Té la paraula.

José Navarro Hernández (perit informàtic)

Molt bé. Bé, moltes gràcies. Bon dia. Soc en José Navarro i treballo com a pèrit informàtic. La nostra experiència en aquest cas ha sigut treballar en el context de processos judicials, de portar prova a processos judicials en els quals hi ha sospites de que certs telèfons mòbils han pogut ser compromesos amb *software* que s'instal·la de manera no autoritzada, en aquest cas *software* de tipus Pegasus de l'empresa NSO.

En aquest context, com que nosaltres hem aportat prova a processos judicials que estan en marxa ara, aleshores, ara no tenim tota la llibertat de portar tota la informació d'aquest tipus de casos, sobretot detalls de qui ens ha contractat o detalls dels resultats concrets d'aquestes anàlisis pericials. Sí que podem dir..., podem contestar preguntes tipus genèriques de com fem les anàlisis, com fan les cadenes de custòdia, com assegurem que els nostres resultats són autèntics, són íntegres i que es poden comprovar, es poden ratificar. I també –que suposo que serà objecte d'interès– com ens hem recolzat en anàlisis prèvies d'altres organitzacions públiques.

Dit això, jo seré molt breu en la meva intervenció perquè jo entenc que és més important les preguntes que puguin tenir i el que pugui respondre, que no fer una introducció genèrica al tema. I jo, per la meva banda, em sobren vint-i-vuit minuts, si volen fer preguntes. També he d'aclarir que normalment, com a pèrits informàtics, la nostra feina la ratifiquem a judici i la nostra manera de treballar és aquesta. Ens veiem sotmesos a les preguntes de les parts i del jutge, o sigui que estem més còmodes en aquest format.

El president

Molt bé. Doncs si els grups parlamentaris volen fer preguntes, requeriments. Comença vostè, senyor Aparicio?

Oscar Aparicio Pedrosa

Bé, bon dia, moltes gràcies. La veritat és que esperava alguna mena d'explicació *(l'orador riu)*, no així entrar *a saco*, sense explicació, però en tot cas, bé, jo m'havia preparat algunes preguntes. Li haig de dir que vaig estar escoltant i llegint el bloc que fan i el pòdcast que fa la seva empresa i el vaig trobar molt interessant; sobretot aquí, en aquesta comissió, que la majoria som advocats, la veritat és que és molt interessant.

I respecte al que vostè ha comentat de la seva experiència, a mi m'agradaria que... Bé, començaré per una altra part. Vostè diu que ha tingut contacte... No sé, sense dir la persona, si ha tingut alguna experiència amb algun de les persones afectades. No sé si ens ho pot dir o no, però en tot cas crec que seria interessant, sense dir el nom, si n'ha tingut amb alguna de les persones presumptament afectades o que surten en l'informe de The Citizen Lab.

A mi també... En un dels seus blogs i dels seus pòdcasts parla de la cadena de custòdia. A mi m'agradaria també que ens expliqués, en el cas en concret, no en general, sinó el cas en concret, en un presumpte espiament d'una terminal per part de Pegasus, com es respecta la cadena de custòdia.

Després, una altra pregunta que també em va venir escoltant el seu programa és respecte a..., perquè hi ha persones presumptament afectades que diuen que no volen entregar les terminals, perquè allà hi ha tota la informació, no només la que està relacionada amb la seva esfera política.

Vostès, en un dels seus peritatges, al blog, comenten que han tingut experiència de fer una contra pericial extraient-ne només part, o sigui, el contingut que de veritat els interessava. I a mi m'agradaria saber si, en aquest cas, en el cas Pegasus, també es pot fer així, és a dir, es pot fer un contrainforme o un contraperitatge sense haver d'accedir a la totalitat de la informació que hi hagi en aquella terminal.

També respecte al tema de Pegasus, una de les qüestions que hi ha hagut, no només aquí a Espanya, sinó en altres països, és el tema dels falsos positius. A mi m'agradaria saber si segons la seva experiència és fàcil o no és fàcil que es donin falsos positius, per què es produeixen i com es produeixen.

També respecte a una de les qüestions que jo entenc..., llegint –evidentment, jo soc advocat, per tant, de temes informàtics no hi entenc– altres informes que qüestionen la metodologia de The Citizen Lab parlen molt de l'eina que utilitzen, l'MVT, em sembla que es diu, aquella eina. M'agradaria saber si vostès l'han pogut analitzar aquesta eina i, si ho sap, si ens pot explicar una miqueta com funciona. Perquè en algun cas he llegit que funcionen posant uns ítems previs, és a dir, mirant el terminal que es connecta a determinades pàgines, si això és així o no i si ens ho pot explicar una miqueta.

També a mi em va semblar dels primers informes de The Citizen Lab que deien que tots o la majoria d'aquests presumptes espionatges es feien a través d'una vulnerabilitat que tenia WhatsApp, però després no coincideixen o com a mínim sembla que no coincideixen les dades en què hi havia aquesta vulnerabilitat amb les dades en què presumptament estaven espiats.

Llavors, en algun cas també he llegit el tema de que es necessitava un missatge, o no es necessitava un missatge per poder infectar la terminal. M'agradaria saber si creu que es pot fer sense aquest missatge. Si de la seva experiència, a part de Pegasus, coneix si hi ha d'altres empreses que també tenen aquesta tecnologia del *zero click*, em sembla que es diu, és a dir, que es puguin infectar terminals sense necessitat de prémer cap *link*, cap enllaç, etcètera.

No sé jo la seva experiència respecte a l'informe de The Citizen Lab, si la puc llegir, totes les versions que hi ha. En tot cas, què li sembla, si se l'ha pogut llegir, el fet de que n'hi hagi algunes que no hi estigui predeterminat quines són les persones o que hi hagi aquestes qüestions que a vegades posa que no se sap o no es pot extreure quina és la data d'infecció. Si això és normal, o per què pot passar això?

Llavors si de la seva experiència també que ha dit que té en el programari Pegasus, si..., a veure com ho direm, això. A veure, d'aquesta experiència que vostè té, com es pot atribuir d'on ve l'origen d'aquesta infecció. És a dir, qui és el culpable o el responsable d'aquesta infecció. Si això es pot fer o es pot determinar mirant les anàlisis des de les terminals. Si es poden fer totes aquestes atribucions –em quedaré sense temps, eh?, ja l'hi faré arribar per escrit, en tot cas, si després és tan amable de fer-ho– si es pot fer aquesta anàlisi sense tenir la terminal, és a dir, només amb les dades que es pogués treure de les metadades, etcètera, si es pot fer.

També, si vostè ho sap, com es fa aquesta anàlisi? És a dir, s'agafen telèfons a l'atzar i es pot veure en tots els telèfons, en aquests i, per tant, es pot determinar qui l'ha tingut o qui no el té, si encara està vigent o no està vigent; si es fa també a través d'això que li explicava, que a mi m'ha sembla que és així, el tràfic de dades. Si és només així o hi ha alguna altra evidència mirant la terminal que es pugui fer, que es pugui saber.

Llavors, si ha llegit l'informe de The Citizen Lab, com valora el fet que hi hagi aquestes diferents versions. Ho dic no tant de fons, que també, sinó també de forma, vostè que és pèrit judicial. Com ho podem valorar, el fet de que hi hagi tantes versions diferents? I, per tant, què s'hauria de fer per donar-li encara més validesa o més integritat en aquest informe? Si aquest programa de l'MVT és l'únic que existeix al mercat o hi ha altres programes, també ens agradaria saber-ho. Si... Bé en tot cas, com que se m'ha acabat el temps, ja li faré arribar per escrit o si no, si hi ha un segon, ja continuaré amb les preguntes.

Gràcies.

José Navarro Hernández

Intentaré més o menys... Perdó.

El president

Vol contestar vostè? Normalment ho fem per als grups, però si vostè ho prefereix...

José Navarro Hernández

(Per raons tècniques, no han quedat enregistrats els primers mots de la intervenció de l'orador.) ...molt semblants a la resta, com vostès vulguin.

El president

(El president intervé sense fer ús del micròfon.) Ho fem així. Com que no ha fet introducció, contesti i després...

José Navarro Hernández

Sí, a veure, intentaré fer memòria una miqueta, si no ho tenim aquí apuntat. Hi han moltes respostes que jo crec que respondran a diverses preguntes.

Primer, nosaltres hem fet anàlisis als terminals mòbils de diferents persones i tenim un grup estadísticament representatiu. Tenim entre quinze, vint persones, és a dir, a diferents..., o sigui, com ho fa Citizen Lab o Amnistia Internacional? Tenim la imatge de cadascuna de les terminals, però també tenim una visió transversal de com funciona aquest sistema, veient en el conjunt com són tots els resultats. Això respecte a la primera pregunta que comentava sobre les persones, el número de persones; la nostra anàlisi no es limita només a un terminal mòbil concret en un moment concret.

La següent pregunta crec que era sobre la cadena de custòdia. I això és molt important, perquè, de fet, contesta una altra pregunta que ve després. Nosaltres, com a perits informàtics, aportem mitjà de prova a un procés judicial. Això, què significa? Que ha de tenir una validesa legal davant d'un tribunal. I aquesta potser és la major diferència entre la nostra feina i la feina que potser han fet Citizen Lab i Amnistia Internacional.

Veient com s'ha tractat aquest tema a premsa i en algunes altres compareixences, algunes crítiques que s'han aixecat, s'ha de pensar que Citizen Lab o potser Amnistia Internacional no han fet la seva feina més des d'un punt de vista científic i, per tant, no podien esperar el 2015 o el 2016 que això pogués acabar en un procés judicial. I llavors les cadenes de custòdia i tot aquest tipus de garanties formals no estan presents als seus estudis.

Per això, entrem nosaltres. Nosaltres sí que hem fet una cadena custòdia dels terminals, de tota la informació que hem pogut agafar, és a dir, no és només de la part que sabem que és important per identificar Pegasus, sinó que hem intentat sempre agafar tot el que han pogut de cadascun dels terminals.

Llavors, responent una altra pregunta, hem agafat tot el terminal, part del terminal. Això depèn una miqueta de la persona, és a dir, nosaltres, evidentment, quan una persona física ens ve amb un terminal per fer una anàlisi, nosaltres informem de que la cadena de custòdia sempre és millor fer-la de tot el dispositiu. Per què? Perquè tot i que la nostra anàlisi sigui d'una petita part, nosaltres com a pèrits actuem en un procés que pot anar a judici. I l'altra part en aquest procés té el dret fonamental de fer una contrapericial. Aquesta contrapericial la farà un altre pèrit i nosaltres no sabem el que farà l'altre pèrit. Llavors, si nosaltres fem només una part, doncs, l'altre pèrit pot dir: «Escolta, jo no puc fer l'anàlisi ics, perquè l'altre pèrit no ha fet la cadena de custòdia completa, per exemple.» Llavors nosaltres sempre recomanem: com més gran millor.

Evidentment hi ha persones que no volen, pel que sigui. Tothom té telèfons mòbils, i llavors és fàcil entendre que no és el mateix que fer una còpia d'un ordinador, perquè hi ha molts més efectes personals a un telèfon mòbil. Llavors, en aquests casos hem fet, doncs, una cadena de custòdia més petita. Això és crític, no crític? Això dependrà de cada cas particular. No és crític en la visió transversal de tot, perquè la visió transversal de tot sí que tenim còpies senceres de suficients mòbils per tenir confiança en els nostres resultats.

Responent una altra pregunta: què caldrà per fer una contrapericial? Això ho haurà de dir el contrapèrit. Entenem que la contrapericial de la nostra anàlisi l'haurà de fer algun cos públic, entenc jo que Mossos d'Esquadra, no ho sabem. I sabem com funciona Mossos d'Esquadra, treballem molt amb ells, i segurament intentaran tenir accés a tot el telèfon mòbil per fer la seva anàlisi. Suposo que les persones propietàries dels telèfons no tindran problemes amb això i es pactarà. Hi ha solucions per fer-ho.

O sigui, ja comentava que nosaltres ja ho tractem en el nostre pòdcast i després a processos concrets, però hi ha maneres de que l'altre pèrit pugui tenir accés a tot el contingut del dispositiu que s'ha de contraperitar, però amb garanties de que informació que no és rellevant per al cas sigui accedida en aquesta contraanàlisi. Hi ha maneres de fer-ho, hi ha moltes maneres de fer-ho. O sigui que aquest punt no em preocupa, no ha de preocupar molt.

(Veus de fons.) Bé, això és més o menys lo mateix. Parlàvem del tema de l'eina de Citizen Lab, d'Amnistia Internacional, de l'MVT. Això és una eina que va desenvolupar Amnistia Internacional basant-se en la informació pública del troià Pegasus. Com funciona la detecció en general d'un programa maliciós? El que normalment fa un programari maliciós quan infecta un terminal o un dispositiu, ja sigui Pegasus o qualsevol altre, és intentar ser invisible. Normalment un troià intenta fer això.

El que passa és que això és molt complicat, perquè en un sistema digital, doncs, qualsevol activitat pot deixar un rastre i la nostra feina com a informàtics forenses normalment és buscar aquests rastres. Quan tu tens un terminal que tu saps que ha sigut infectat amb un sistema d'aquest tipus i, en els primers casos, tant d'Amnistia Internacional com de Citizen Lab, es sospitava això per..., bé, podem entrar en detalls, però els seus informes ho deixen bastant clar, que ells tenien moltes sospites de que els seus terminals estaven infectats. El que van fer és una anàlisi d'activitat

per veure quins rastres que no són típics en un telèfon normal es generaven en aquest telèfon. Llavors, veient un cas, l'altre, l'altre, l'altre i sobretot veient com es comunicaven amb internet, doncs, vam poder establir un patró de comportament d'aquest tipus de *software*.

Els patrons dels comportaments, per exemple, en el cas Pegasus i tal com està descrit als articles de Citizen Lab públics, i Amnistia Internacional i nosaltres també ho hem pogut confirmar, hi ha dos tipus de patrons. El primer tipus de patró és l'activitat que es genera a dins del telèfon. Per exemple, quan tu tens un programa a un terminal mòbil que intercanvia dades amb internet, això deixa un registre, una base de dades del telèfon perquè... Les persones que són usuàries d'iPhone, per exemple, saben que hi ha una part del telèfon on et diu quin és el consum per aplicació, per exemple, de dades mòbils, wifi i tal per tenir una miqueta de control.

Doncs aquest registre deixa guardat el nom dels processos, els programes informàtics que estan corrent i que estan intercanviant informació a internet. Doncs hi ha noms de processos que semblen processos del sistema però no són exactament igual. Tenen alguna lletra diferent i això és un típic marcador de que hi ha un programa que intenta ser invisible fent-se passar per un autèntic. Com que no pot utilitzar el mateix nom, n'utilitza un de molt semblant perquè a aquella persona, instal·lador de sistemes o el que sigui, que vegi això, doncs, no li soni estrany. Mirant aquest tipus de registres, doncs, pots fer un patró del programa que està infectant. Hi ha molts noms de processos que s'han identificat a terminals que sabem que han sigut infectats amb aquest sistema Pegasus d'NSO.

El segon tipus de patró de comportament és com es comuniquen amb internet. Aquí hi ha la fase d'infecció, és a dir, el telèfon s'infecta a través d'internet i per això hi ha vegades que fa una comunicació activa amb un servidor d'internet, amb una pàgina web, etcètera, i això deixa un registre, per exemple, a l'historial de navegació. O, per exemple, si aquesta navegació ha sigut motivada perquè s'ha rebut un SMS amb un enllaç i l'usuari ha fet clic, doncs, aquest SMS es guarda al telèfon. El troià Pegasus esborra coses de la seva activitat però no esborra els SMS. Llavors veiem els SMS, els enllaços a internet. Podem veure a quin servidor s'ha connectat.

I Citizen Lab va fer molt bona feina identificant, associant, perdoneu, aquests servidors d'internet amb servidors coneguts d'NSO. Això és una part supercrucial d'aquest informe. Perquè després, quan es van publicar els primers resultats, a conseqüència d'això, NSO va començar a amagar els seus servidors. Però com que Citizen Lab ja en coneixia alguns, va poder fer un seguiment de com canviava la manera de reconèixer aquests servidors a internet i ha pogut fer un seguiment fins avui en dia.

Llavors, primera part, tenim clar quin és el *software* que s'executa als terminals mòbils i dos, tenim l'associació amb NSO per aquesta associació de comunicacions amb internet. Crec que això... I l'MVT, al final, el que fa és només fa una miqueta de mira quins són els noms dels processos i dominis d'internet i adreces de correu electrònic que s'han identificat en casos de Pegasus. És l'únic que fa. Llavors, hi ha hagut crítiques de com funciona MTV i com pot generar falsos positius, que és una altra pregunta. Això és una miqueta..., per a mi és una miqueta... Se n'ha parlat massa, perquè evidentment un programa que et baixes gratis d'internet, que et mira noms de processos i dominis, evidentment no pot, no es pot fer servir com a prova definitiva de re.

Nosaltres, per exemple, als nostres informes pericials, el que hem fet és executar l'MVT, veure que surten coses, però després hem anat directament als telèfons mòbils i hem buscat aquestes coses i hem mirat en quin context apareixen, si són coherents o no amb altres indicadors, com apareixen en el mòbil. Hem reconstruït l'activitat a cada telèfon mòbil de tots aquests indicadors de compromís, per veure si és coherent o no.

Per exemple, hi ha programes a internet que el que fan és injectar un telèfon en blanc als indicadors de compromís, perquè quan tu passis l'eina d'Amnistia Internacional et digui que és un fals positiu, no? Doncs evidentment, quan tu fas aquest tipus d'injecció, la manera d'injectar aquests indicadors de compromís és molt..., es veu fàcilment que és fals i no té molta coherència. Llavors, la resposta és que amb una anàlisi profunda sí que es pot veure, es pot discriminar si els resultats de l'MVT poden ser falsos positius o no.

Responent a una altra pregunta, nosaltres el que veiem és que en alguns casos dels nostres telèfons que hem analitzat arribem a conclusions lleugerament diferents a les quals arriba Citizen Lab. Per exemple, hi ha vegades que Citizen Lab sí que considera que un telèfon ha estat afectat en una data concreta, infectat a una data concreta. I nosaltres, mirant el telèfon, veiem que aquest telèfon sí que ha rebut SMS maliciosos, però no veiem després els indicis d'infecció; i al revés. Per què passa això? Perquè quan... En un dispositiu electrònic digital, és important saber que sí que és veritat que tota activitat deixa molt de rastre. Això és un avantatge per fer una anàlisi forense, però després aquests indicis s'eliminen amb el temps. Llavors, el que tenim ara, mesos o anys després, és una visió molt segmentada. Llavors, hem de reconstruir. Hi ha vegades que veiem l'SMS, però no veiem indicis d'infecció. O sigui que no podem concloure que hi hagi hagut infecció. I altres en casos està molt clar.

I crec que això respon amb moltes de les preguntes. Com que m'he passat molt de temps, potser és millor...

El president

No, jo penso que anirem refent. I si el senyor Aparicio en té alguna que no..., la torna a formular o els hi fem arribar, si a vostès els sembla bé, per escrit, i...

José Navarro Hernández

Cap problema.

El president

...les passarem a tots els membres del comissió. Següent grup. No fem cap ordre, ens organitzem. Tu? Senyor Rius...

Josep Rius i Alcaraz

Bé, doncs, molt bon dia i moltíssimes gràcies per venir aquí i fer una cosa que nosaltres estem mirant de fer, que és posar –i fem servir aquesta expressió també– «una miqueta de llum en una foscor», és a dir, en un espionatge modern. De fet, la tecnologia ha permès sofisticar molt, diguem-ne, l'espionatge tradicional que s'havia fet fins ara i, per tant, doncs, també els volia traslladar, diguem-ne, aquesta magnitud històrica que també té el que estem mirant de fer des del Parlament de Catalunya i que, malauradament hi ha altres cambres, com el Congrés dels Diputats, que es neguen a investigar.

Jo li volia fer algunes preguntes en bateria, i miraré de ser ràpid. També si pot fer breument una miqueta quina experiència professional tenen vostès i quants anys tenen, diguem-ne, duent a terme peritatges judicials. La segona de les preguntes, si me la pot respondre, és, per la seva experiència, si poden tenir algun tipus d'intuïció de qui pot adquirir aquest tipus de programaris i quins usos s'hi acostumen a fer, amb quina intencionalitat?

La tercera de les preguntes és si saben, pel sistema de funcionament d'aquest programari, tant de Pegasus com també de Candiru, si aquestes dades, posem pel cas i posem la hipòtesi de que això ha estat fet per un organisme estatal –l'Estat espanyol– si aquestes dades, que són dades personals, personalíssimes, de fet, que poden afectar, diguem-ne, tant la privacitat, les comunicacions, el secret professional, etcètera, si romanen només a l'Estat espanyol o també van amb un servidor i, per tant, van a un altre país. En aquest cas podria ser, per exemple, Israel, on NSO té la

seva seu. Ho dic també per les connotacions que això té que unes dades d'aquestes característiques surtin del control d'uns serveis secrets o d'un organisme estatal.

En quart lloc hi ha, i aquí presents, persones que han qüestionat el rigor científic de Citizen Lab, de la Universitat de Toronto, i si creu que Citizen Lab actua amb professionalitat, amb un rigor científic, que l'acrediten, al meu entendre, els seus més de vint anys d'experiència professional.

En cinquè lloc, quina capacitat tenen aquests programaris Pegasus i Candiru? És a dir, què poden arribar a fer, segons el seu entendre: poden monitorar totes les dades, poden activar un micròfon, poden activar la càmera? Poden arribar a modificar, editar, afegir, suprimir dades, correus electrònics, fotografies, etcètera, tot el que els terminals actuals tenen capacitat, diguem-ne, de poder fer?

En sisè lloc, és òbvia, però li haig de fer aquesta pregunta: creu que pot acreditar en el seu peritatge judicial que un mòbil ha estat infectat amb Pegasus o Candiru i esdevenir una prova judicial d'acord amb l'ordenament jurídic vigent?

I, en darrer lloc, si poden acreditar tant els intents d'infecció com les infeccions efectivament utilitzades. I, per últim lloc, si poden arribar a saber també d'alguna manera, aquesta cadena, si aquestes dades poden haver passat per diferents servidors, si poden arribar vostès a saber-ho.

El president

(Per raons tècniques, no han quedat enregistrats els primers mots de la intervenció de l'orador.) ...i encara tens...

Joaquim Jubert Montaperto

Sí; jo, tres preguntes, senzillament. Durant quant de temps es poden mantenir les dades en un telèfon punxat; o sigui, es pot recuperar la informació sobre un telèfon que ha estat punxat? Durant quant de temps? Es pot esborrar? La probabilitat d'encert sobre un mòbil infectat, o sigui, realment es pot..., quina probabilitat d'encert per l'avaluació? I després, seguint el rastre d'un servidor on van a parar les dades, es pot saber el beneficiari últim d'aquestes dades?

José Navarro Hernández

Gràcies. Bé, llavors, responc primer a la primera pregunta i després farem les últimes, perquè tenen més relació i jo crec que de les intermèdies alguna ja quedarà contestada.

Primer, nosaltres som perits informàtics especialitzats en informàtica forense. Tenim la nostra empresa, Evidentia, que treballa des de l'any 2000. Tenim molta experiència en tot tipus d'anàlisis forenses de telèfons mòbils, ordinadors, pàgines d'internet, en tot tipus de casos socials, civils, penals, inclús administratius. Però bé, això està dins del nostre currículum i, al final, cada informe i cada prova, segons la meva opinió, s'ha de mirar individualment, per la prova i pel que s'aporta, no pel currículum de pèrit.

Segon, sabem que l'índex de probabilitat d'infecció d'un telèfon és bastant alt. Per què? Perquè nosaltres, de tots els telèfons que hem mirat, podria dir que el noranta per cent tenien infeccions confirmades. Clar, això pot tenir..., estadísticament pot ser no molt imparcial, perquè, clar, les persones que ens han aportat els telèfons ja tenien molta motivació per saber que ja estaven infectades i moltes ja havien fet una anàlisi prèvia amb Citizen Lab. Però jo crec, veient una miqueta la manera d'infectar d'aquesta empresa, que hi ha molta probabilitat que siguin reeixides les infeccions. Per què? Perquè a NSO, com totes, hi ha una tradició; en el món de la seguretat informàtica ja han sortit moltes empreses i molts productes d'informàtica forense d'Israel, per alguna raó, i està molt demostrat que les empreses israelianes tenen molt coneixement dels sistemes operatius de Microsoft, d'Apple...

Per exemple, nosaltres utilitzem un *software*, un sistema per fer anàlisi de telèfons mòbils que és legal i que s'utilitza de manera privada i pública i que fa servir vulnerabilitats conegudes per accedir al telèfon i extreure dades. Això públic, o si-

gui, lo que es faci després per sota la taula, doncs, és bastant creïble que sigui més. És molt públic també, i assumit, que hi ha empreses que ofereixen aquest tipus de serveis només a governs i només a cossos i forces de seguretat d'estat. Per exemple, altres tipus d'empreses tenen dues modalitats de producte: una, la que ofereixen a persones com nosaltres, que són privades, pèrits privats, i després altres tipus de versions del mateix producte que ofereixen a cossos de seguretat, que ofereixen més coses.

Llavors, podem confirmar que sí que ja és completament indiscutible que aquest mercat existeix i que hi ha certs productes que només s'ofereixen a aquest tipus d'organitzacions. De fet, també és públic que Israel considera els productes d'NSO com una arma i que, per això, es requereix una autorització per part del Govern d'Israel per vendre els productes d'NSO fora d'Israel; això tampoc ha estat negat per ningú.

En aquests dos minuts, hi havia una pregunta més de... *(Veus de fons.)* Ah, sobre dades personals i sobre per on van les dades. Nosaltres, amb el nostre informe, amb resultats diferents als que ha tingut Citizen Lab, podem confirmar un resultat al qual també arriba Citizen Lab, en el cas concret del que s'anomena el «Catalangate», que és que molt probablement la infraestructura de Pegasus que es va utilitzar en aquest espionatge va ser instal·lada fora de la infraestructura d'NSO.

És a dir, NSO se sap que té la modalitat d'oferir Pegasus des de la seva infraestructura, però també pot posar, diguem-ne, un armari d'ordinadors a la teva oficina on ells posen els ordinadors i tu des d'allà fas el que hagis de fer. I Citizen Lab ja ho diu, bé, ho deixa entreveure a un dels seus informes, que el patró d'identificació dels servidors utilitzats en el «Catalangate» és lleugerament diferent al que havíem vist. I això es pot interpretar com que és una infraestructura *ad hoc* que està darrere d'un tallafocs o alguna infraestructura de seguretat diferent a la resta.

Però nosaltres, de la nostra versió transversal, hem tingut un altre resultat que ens ve a dir lo mateix. És a dir que probablement la infraestructura utilitzada per tots els telèfons del «Catalangate» segurament era una infraestructura dedicada d'una mateixa organització. A on van les dades? Això és un gran misteri i no sabem molt bé això com funciona. Segur que aquesta infraestructura dedicada s'emmagatzema amb dades, segur. El que no tenim clar és a quines dades té accés NSO i quines dades van fora d'aquesta infraestructura cap a, per exemple, una infraestructura israeliana. Això no ho sabem.

Com que m'he passat de temps, no sé... Queda lo de les funcionalitats. Són molt públiques. Aquí l'únic que diré és que el punt important d'un *software* com Pegasus no és el tipus d'informació que pugui extreure dels telèfons, perquè hi ha programes que corren per internet gratuïts des de fa molts anys que són troians molt potents que fan extracció d'SMS, converses, t'activen el telèfon, fan intercepció de comunicacions, fan moltes coses. Això són *softwares* que corren per internet i que estan gratuïts.

El punt fort de sistemes com Pegasus i d'empreses com NSO és que poden instal·lar aquest tipus de *software* de manera no autoritzada a un telèfon. És a dir, jo puc agafar un troià d'aquest tipus i instal·lar-lo al meu telèfon, perquè jo soc administrador del meu telèfon i el vull instal·lar per fer proves, per exemple. Però com l'instal·lo al telèfon d'ell, si ell no em dona autorització? I com ho faig perquè ell no se n'adoni? Aquest és el punt clau.

Llavors, funcionalitats del troià? Moltes, moltes. Pot modificar el contingut del telèfon? La nostra anàlisi demostra que sí. Nosaltres hem vist que el patró de comportament de Pegasus canvia amb el temps. Les versions més modernes, per exemple, esborren certs registres de la base de dades del telèfon perquè NSO sap, pels informes de Citizen Lab i Amnistia Internacional, que es fan servir com a indicadors de compromís, però ho fan també d'una manera grollera i, bé, el pots associar amb l'activitat de Pegasus, però veiem que poden manipular, evidentment, el contingut del telèfon.

S'ha debatut molt sobre si Pegasus pot injectar, per exemple, informació que es pugui fer servir com a prova, és a dir, SMS que no existien... Això nosaltres no ho hem vist, no sabem... Pegasus té una finalitat que no és aquesta. Teòricament podria ser, evidentment, però no. Nosaltres hem vist que sí que modifica el telèfon, però només amb la intenció d'amagar els seus rastres. O sigui, esborra bases de dades amb els seus rastres.

I sobre la validesa del nostre informe, al final nosaltres intentem aportar els informes amb totes les garanties legals que un pèrit informàtic ha de fer servir. I aquesta qüestió l'ha de decidir un jutge. El jutge, al final... Nosaltres fem un peritatge; l'altra part fa un altre peritatge, i és el jutge qui decideix si confia, si no confia, si és vàlid o no és vàlid.

El president

Moltes gràcies, senyor Navarro. *(Veus de fons.)* Doncs Jordi, endavant, senyor Orobitg.

Jordi Orobitg i Solé

Moltes gràcies. Si m'ho permet, voldria fer una prèvia. L'altre dia vam tenir l'oportunitat de desplaçar-nos fins a Madrid, en aquest cas, per intercanviar opinions i que els portaveus d'aquesta comissió poguessin expressar, doncs, el parer d'aquesta comissió respecte a la investigació que s'està duent al Parlament Europeu. I voldríem posar en valor i agrair en qualsevol cas a la Mesa que adoptés la decisió de posar en coneixement de la Mesa del Parlament el fet de que som administradors de recursos públics i, en aquest cas, un representant d'una formació política que va voler fer aquest viatge, desplaçar-se amb tota la comissió per comparèixer davant del Parlament Europeu, no ho va fer i, en definitiva, va utilitzar aquests recursos públics per fer un ús partidista i interessat, doncs, d'aquella comissió. I, per tant, perquè entenem que se'n va fer un mal ús, d'aquests recursos, agraïm, des del nostre grup parlamentari, volem agrair, la fermesa d'aquesta Mesa en posar-ho en coneixement dels organismes adients perquè es reintegri en qualsevol cas la despesa la despesa pública que el seu desplaçament va comportar.

Dit això, amb caràcter previ, agrair en tot cas la compareixença. Valorem, doncs, l'honestedat i el plantejament que se'ns fa, perquè crec que és molt rigorós. En aquest cas se'ns explicita que, a diferència de Citizen Lab, que fa un estudi forense amb relació a una sèrie de circumstàncies, el que fan també és un estudi forense, però adreçat en aquest cas a un procediment judicial i que, per tant, se li exigeix un màxim rigor no només perquè es posa en qüestió la seva praxi i el seu coneixement, sinó també el seu propi prestigi professional.

I, per tant, crec que és molt rellevant, doncs, que les conclusions que ens han expressat i amb la fermesa que ho han fet, crec que avalen –no crec, avalen– quelcom que per a molts de nosaltres és incontestable, que és l'ús espuri d'una eina, un *spyware*, un *software*, d'una forma no avalada o no acceptada, en aquest cas, per l'usuari del terminal, amb una finalitat també espúria ja que, pel que vostès mateix expliciten, hi ha un nombre d'infectats molt elevat, que és molt més elevat que no aquell que des de part del Govern espanyol s'ha acceptat, que ha estat avalat per una autorització judicial, no?

Jo, el que em sembla rellevant del que han dit és que vostès arriben a aquesta conclusió en funció de la gran mostra de terminals que han tingut la possibilitat, des del punt de vista de forense, d'analitzar. I, en aquest cas, sí que els hi agrairia que em determinessin quin és el nombre exacte de, en aquest cas, terminals que han pogut examinar i també voldria que ens determinessin si les seves conclusions respecte de la praxi de l'anàlisi de tots aquests terminals són..., o la praxi per arribar a les conclusions és diferent de la d'Amnistia Internacional i també de Citizen Lab. I per a nosaltres és important perquè, com bé s'ha dit abans, el tema dels falsos positius és rellevant, perquè és l'eina que per qui qüestiona la realitat d'aquest espionatge s'uti-

litza i ho fan també, en aquest cas, amb fonament, en aquest cas en informes, no?, com podem conèixer, que en aquest cas es va defensar davant de la Comissió del Parlament Europeu pel senyor Gregorio Martín Quetglas, que qüestiona, en aquest cas explícitament, l'informe de Citizen Lab i, per tant, voldríem... Ja sé que ara no es tracta de fer una contrapericial en seu parlamentària, però home, crec que és important o rellevant, per a nosaltres ho és, que si existeixen tres praxis diferents, tres procediments diferents de determinació d'aquesta infecció, doncs, que vostès ens les puguin explicitar si entenen que aquests dos altres mecanismes, el d'Amnistia Internacional i Citizen Lab arriben a les mateixes conclusions que vostè.

Des del Parlament, hem tingut o vam tenir un debat important i vam arribar a un acord majoritari a la cambra per adreçar-nos al Parlament Europeu, doncs, demanant-li que adoptés una sèrie de mesures respecte a aquesta circumstància, perquè tenim el convenciment que aquest espionatge ha existit i que s'ha focalitzat en un col·lectiu determinat, que és el de l'independentisme. I vam tenir un debat molt important sobre si havíem de demanar al Parlament Europeu que s'adoptessin mesures per regular, en aquest cas, la utilització de Pegasus o altre *spyware* o que es procedís a la seva il·legalització, és a dir, que comminés els estats membres a que no es pot utilitzar.

I la meva pregunta és, des del seu coneixement, des de la seva experiència, si vostès entenen que és factible que es pugui produir un ús limitat d'aquestes eines, és a dir, mentre existeixi una autorització judicial, es pot sectoritzar o fer un compartiment explícit i determinat de l'accés a dades determinades del terminal o qui ho fa evidentment pot accedir a la integritat del terminal. I com bé ha dit vostè, les pròpies recances de les persones infectades a cedir el seu mòbil, perquè conté el noranta-cinc per cent de la informació personal d'una persona: els seus contactes, les seves fotografies, les seves cites, les seves converses i, per tant, és evident per un pudor personal, no?, que existeix aquesta limitació a cedir aquests terminals. Per tant, vostès entenen que això es pot regular? O directament s'hauria d'advocar en aquest cas per la il·legalització?

I en segon lloc, vostès entenen que el tràfic d'aquestes dades, aquest intercanvi de dades en diferents servidors... S'ha qüestionat si es trobaven en territori de l'Estat espanyol. Semblava que pel que vostès diuen podria ser, perquè s'ha creat una infraestructura *ad hoc*. Però quin tipus de garantia pot tenir ningú que amb una infecció avalada o no judicialment no trobarà el dia de demà a la *dark web* totes les seves dades personals penjades i de lliure accés per a qualsevol tercer, amb l'ànim de voler destruir personalment..., tenint en compte que estem parlant d'accessos no regulats per cossos, moltes vegades serveis secrets, que no tenen..., *a priori* no es veuen limitats, doncs, pels drets constitucionals de les persones a l'hora de garantir la seguretat nacional.

Moltes gràcies.

El president

Gràcies, senyor Orobitg. Senyor Navarro.

José Navarro Hernández

D'acord. Primer, per contestar aquesta última pregunta, que em sembla molt interessant, primer has de recordar que jo no soc advocat. Sabem coses de dret, perquè ja portem molt de temps, però jo sempre he dit que si alguna cosa que dic, un advocat diu que no, és que no. Sobre la utilització d'aquest tipus de sistemes, la seva legalitat, la seva limitació, la seva... O sigui, jo, com a persona que no soc advocat, no em puc pronunciar, però s'ha de recordar que el Codi penal i la llei d'enjudiciament criminal ja suporten des de fa molt de temps la intercepció de comunicacions, quins requisits ha de tenir, la tutela judicial d'aquestes comunicacions, com s'han de protegir, durant quant de temps, quant de temps el jutge ha de renovar... És a dir, esta molt controlat, això.

De fet, des de l'última reforma del Codi penal, el que s'ha fet és ampliar. O sigui, hi ha confiança en aquest sistema i s'ha ampliat. Hi ha la figura del policia encobert, s'autoritza, de fet, policia judicial, evidentment amb supervisió judicial, a instal·lar programari d'aquest tipus en terminals per obtenir informació. Ara no ho recordo exactament, però crec és que en casos ja molt greus i estan establerts, etcètera. O sigui que hi ha un marc legal per fer això.

Si és legal o no Pegasus, això ja jo no ho puc dir, però podria ser-ho. O sigui, nosaltres, per exemple, hem fet contrapericials d'intervencions policials de veu, de dades i tal, i es fan servir sistemes que, de fet... Ara parlo de memòria, eh?, però crec que el sistema que es fa servir per a les interseccions digitals va ser comprat pel Ministeri d'Interior a Israel. O sigui que, és a dir, en aquest sentit, jo entenc que es podria fer.

Sobre quin risc hi ha que aquestes dades es publiquin a la *dark web* i tal, doncs, jo entenc que la mateixa probabilitat i el mateix risc que hi ha amb els sistemes d'intercepció telefònica existeix des de fa anys. O sigui que no crec que lo preocupant d'aquest cas sigui això. Entenc que si està ben protegit, no hi hauria d'haver cap problema. Quin és el problema aquí? Que –i aquí ja parlo una miqueta..., sortim una miqueta del meu àmbit com a pèrit– el problema està en que si els sistemes d'intercepció telefònica i de dades aprovat pel Ministeri d'Interior tenen una regulació, es coneixen, etcètera, el sistema Pegasus no.

Llavors bé, aquí no sabem on està aquesta infraestructura d'NSO. Sabem amb molta seguretat que probablement està a Espanya, però no sabem on és, no sabem qui l'ha contractat, no sabem qui l'ha guardat, no sabem quines mesures de seguretat té. Evidentment, tota aquesta part en altres sistemes d'intercepció que sí que té el Ministeri d'Interior, doncs, sí que està regulada i es coneix i la gent no pateix per això. Però aquí tenim aquesta manca de transparència.

No sé si queda alguna pregunta més. Abans n'havia fet una primera, veritat? *(Veus de fons.)* Ah, la diferència de metodologia. A veure, nosaltres, evidentment, hem hagut d'utilitzar la metodologia publicada de Citizen Lab i Amnistia Internacional. Coneixem les compareixences al Parlament Europeu del senyor Gregorio..., ara no me'n recordo del cognom. A veure, jo, com que no està aquí el company, no atacaré la seva participació.

Jo crec que la metodologia de Citizen Lab no és perfecta. Es pot criticar, evidentment, però no comparteixo les crítiques del senyor... És que Gregorio..., és que no en recordo el cognom. *(Veus de fons.)* Exacte, el senyor Gregorio Martín. En particular les crítiques que va fer al Parlament Europeu, jo les vaig veure com a tècnic que soc. De la resta no opino, però, com a tècnic, es queixava de falta d'objectivitat en l'anàlisi de Citizen Lab, cosa que jo no comparteixo, però la seva crítica mancava d'objectivitat. És a dir, no deia per què. Jo el dia que toqui criticar l'anàlisi de Citizen Lab li podré dir per què exactament. Per exemple, la seva anàlisi va començar l'any 2014-2015 i nosaltres vam parlar amb Citizen Lab per veure què podíem aprofitar i, per exemple, ells van fer uns escanejos enormes de tot internet per identificar servidors. Evidentment, això no es va fer pensant en que deu anys després s'hauria de fer un judici, i evidentment no hi ha un notari fent aquests escanejos, la qual cosa ha sigut impossible, no hi ha una cadena de custòdia, certes coses.

Però si mira, per exemple, les publicacions científiques d'arreu del món, de qualsevol altre àmbit, hi han moltes publicacions científiques que pateixen de gairebé lo mateix, és a dir, cap científic que investiga el covid, per exemple, fa una cadena de custòdia de la mostra que està fent. Al món científic com es guanya confiança en aquestes comunicacions? Doncs publicant les comunicacions, posant-les a l'abast de tota la comunitat perquè siguin atacades.

Llavors hi ha, a la història científica, molts cassos de publicacions científiques que han sigut atacades objectivament i que altres científics que les han atacat hi han pogut demostrar errors o confirmar que són èxits. Així funciona la ciència des de

fa moltíssims anys. Citizen Lab i Amnistia Internacional han fet això, han agafat les seves anàlisis. Ells no són pèrits, no, no pensen... Són científics. El que han fet és publicar això a internet. I jo no he vist cap crítica objectiva a cap resultat tècnic dels seus informes.

És a dir, per exemple, els noms dels processos que s'accepten o s'identifiquen amb Pegasus. Són noms de processos molt concrets. Estan llistats als *reports* d'Amnistia Internacional. Si busques a internet les úniques referències que hi ha són a Pegasus, és a dir, no es coneixen altres usos d'aquests processos i no hi ha ningú que hagi dit: «No, escolta, és que aquest procés amb aquest patró de comportament pertany a una altra cosa.» Llavors nosaltres hem vist... Nosaltres, per exemple, veiem que hi ha processos d'aquest tipus i intentem mirar a cada informe què fa cada procés. Per què? Per poder dir si és una traça d'infecció o només un intent i hem pogut entendre bastant bé com funciona. O sigui que hem pogut entendre aquesta metodologia de Citizen Lab.

El president

Moltes gràcies, senyor Navarro. Senyora Vinyets.

Montserrat Vinyets Pagès

Senyor Navarro, bon dia. També bon dia al senyor Pujol, que l'acompanya. A veure, coses que ja han sortit una mica i que anem intentant endreçar. Amb relació a l'abast de l'*spyware*, ja li ha comentat el company diputat Rius que –i vostè ha contestat– o entenc que sí, no?, que pot afectar trucades, càmeres, accedir a historials de navegació, Facebook, WhatsApp, Telegram..., entenc que a tot arreu. I jo afegiria també la geolocalització de la persona que utilitza el telèfon, també és monitorable.

En segon lloc, no em queda clar si té aquest efecte que a vegades es diu de teranyina. És a dir, que si algú que ha estat infectat amb Pegasus i es comunica amb una altra persona, s'envien *mails*, Telegram, això té un efecte de saltar com una teranyina a la nova persona.

Llavors, jo li faré preguntes que vostè ja ens ha dit que aquí el problema que tenim és la falta de transparència, que hi ha molta..., és un tema que no es coneix, que no hi ha informació i, per tant, jo entenc perfectament el que diu i, per tant, vostè i jo li pregunto i si me diu que no hi ha informació, no?, que a diferència per exemple d'altres sistemes potser com el SITEL o així, d'interceptació de trucades que sí que coneixem més, però això és una cosa desconeguda. Per tant, que quedi constància a la comissió, doncs, que és un àmbit desconegut.

A on va la informació? Perquè la informació que podem treure del telèfon d'una persona és immensa, és ingent. Aquesta informació, cap a on va?, si es desvia de forma encriptada o de forma directa, si es pot emmagatzemar tota. I, clar, jo m'imagino... Com funciona qui rep la informació, no?, perquè com que hi ha tanta informació i de tanta gent, la persona que rep la informació, inclús potser té un sistema d'alertes que actua en funció de que apareguin paraules clau, o si inclús es podrien activar sistemes d'alerta. Perquè evidentment hi ha un problema de gestionar tota aquesta informació que és tan immensa, no?

Sobre la venda d'aquest producte, potser ja em dirà que no sap la resposta, però què s'imagina vostè que es ven. Es ven una llicència i això et dona dret a uns quants telèfons o...? No ho sé, és que no... A veure si vostè té alguna idea de cap a on podríem anar i quines xifres econòmiques... Què pot costar això? No només la venda d'aquestes llicències, sinó també el tenir tota una sèrie de persones, d'espies, entenc, que s'han de dedicar a garbellar tota aquesta informació que es treu dels telèfons i el monitoratge. Abans ho ha advertit una mica, que deia que l'NSO Group té les dues propostes: una, que sigui el mateix NSO Group que et fa la gestió del material espiat o que en canvi NSO Group et ven el *software*, aquest *software* maliciós, que

inclús he llegit en algun lloc que té un telèfon d'atenció directa, fa inclús cursos de formació a qui ha comprat el material.

I jo li volia preguntar si és complex utilitzar aquest *software* per la persona que... Ara ens posem en la situació d'aquell que està gestionant la informació. És complex això o és senzill? Des de quin any vostè té constància que pot ser que existeixi aquest programari Pegasus, si és des del 2016 o inclús abans? Si, per les formes d'infestació, sempre es necessita internet o podria infectar-se en una situació en què no hi hagués internet. Sembla que la infestació pot ser a través d'enllaços, no?, que ells s'encarreguen de donar una aparença de normalitat a l'SMS, que sigui part de la teva quotidianitat. També diuen que és possible per la instal·lació física o per estar pròxima al telèfon. Bé, si ens pot dir quines formes d'infestació hi ha més.

Vostè també ens parlava de que el noranta per cent de telèfons que se li han mostrat a vostè, doncs, han resultat infectats. Sí que és veritat que la majoria de persones que li han portat els telèfons, ja per circumstàncies ics tot apuntava que podien ser susceptibles de ser infectats. La meva pregunta és: vostè creu que, i a la vista de que en el seu moment WhatsApp va presentar una demanda que es parlava de 1.400 persones infectades... Vostè creu que, de les xifres que hi ha recollides de seixanta-cinc persones infectades, aquestes xifres podrien quedar petites i que la infecció pot haver sigut molt superior a aquesta xifra? Una, la reconeguda pel Ministeri de Defensa, que són divuit persones; l'altra per Citizen Lab, que són seixanta-cinc; si podríem parlar d'unes xifres superiors.

I llavors, si vostè en l'àmbit de l'Estat espanyol –jo perdoni, però amb temes informàtics no estic massa al dia– si en l'àmbit de l'Estat espanyol hi ha... Vostè ha dit abans que Pegasus és una arma, una arma de guerra, no?, reconeguda pel Govern israelià, que té la categoria d'arma i, per tant, està subjecte a tota una sèrie de normativa. A l'Estat espanyol, hi ha empreses anàlogues a NSO Group, que tinguin com a objecte social de l'empresa que es constitueixin per accedir a dies zero, a constantment buscar vulnerabilitats. Hi ha empreses que es dediquen a això com a objecte social? I, si és així, quins indicis ens poden fer pensar que una empresa té com a objecte social, això, no sé si m'explico: per la constitució de l'empresa, què ens pot dir que una empresa ja està feta amb aquest objecte?

Gràcies.

El president

Moltes gràcies. Senyor Navarro.

José Navarro Hernández

Sobre el tipus d'infecció, el que està documentat és infecció per internet. És a dir, al final, l'èxit de Pegasus ve com a conseqüència de tenir telèfons que la gent porta gairebé tot el dia a sobre i que estan permanentment connectats a internet. Les vies d'infecció normalment són o per SMS, és a dir, et forcen a accedir a una pàgina web que aprofita una vulnerabilitat del navegador web o dels motors de *software* que utilitza el navegador web per executar codi de manera no autoritzada. O bé fan servir vulnerabilitats de programes que estan contínuament comunicant amb internet per infectar-te, inclús si l'usuari no fa una acció directa. Estan documentades totes dues coses.

De fet, Citizen Lab va alliberar un informe identificant tres vulnerabilitats greus, molt greus, a Apple en aquest sentit i ho van comunicar a Apple. I Apple primer va comunicar la solució dels tres problemes i just després Citizen Lab va publicar el seu informe, que és normalment com es fa al món de la seguretat. O sigui que d'això n'hi ha prova, funciona així.

Sobre la infecció per proximitat, això implicaria vulnerabilitats a comunicacions curtes tipus Bluetooth, coses així. D'això jo no he vist res, o sigui que en principi no. Però evidentment hi ha casos en què hem vist que, bé, nosaltres no ho hem vist, però que està publicat que hi ha persones que han volgut infectar i no han pogut per

temes ics i el que han fet és infectar tot el seu entorn, per tal de que si aquesta persona parlava amb algú de l'entorn, com que no podia infectar la persona, infectava l'entorn. No és exactament el concepte de teranyina que vostè deia, però la imatge és aquesta.

Sobre la comunicació de dades i qui tutela les dades, això és, o sigui, li puc dir el que ja he dit. O sigui, la manera de treballar d'NSO no la coneixem, però coneixem *software* semblants, per exemple SITEL, SILC... Tot aquest tipus de *softwares* que utilitza el Ministeri d'Interior nosaltres hem vist com funcionen i són senzills d'utilitzar perquè al final l'utilitzen persones, funcionaris que no són informàtics, són persones que tenen, bé, les seves capacitats en una altra àrea i són interfícies fàcils d'utilitzar.

Sobre l'ús de geoposició, configuració d'alerta, etcètera, lo important des del nostre punt de vista és l'accés a les dades. Una vegada que les dades estan en una base de dades, pots fer el que vulguis amb les dades: alertes, seguiments, el que tu vulguis. Això no ho sabem, el que poden fer, però les possibilitats són infinites.

Què hi havia més? *(Veus de fons.)* La venda i el cost, no els coneixem. Nosaltres, per exemple, sabem de *softwares* semblants que el cost sol ser no tan gran com una persona podria pensar basant-se només en pel·lícules d'espies i coses així. Al final són uns serveis informàtics i el que necessiten és el coneixement d'aquestes vulnerabilitats per tal d'accedir al sistema. Per alguna raó històrica que desconec gairebé totes les empreses que es dediquen a això venen d'Israel. Sabem que hi ha altres empreses a altres llocs del món, però que no fan públics aquests serveis. Estats Units, per exemple. Però no ofereixen aquests productes a tot arreu, com ho fa Israel.

El cost no el sabem. El tipus de llicenciament tampoc. Coneixem això, que molt probablement el que hem vist que s'ha instal·lat aquí és una infraestructura *ad hoc*, molt probablement és així. El que no sabem és quin tipus de control té Israel sobre aquest sistema. Nosaltres, per exemple, coneixem *softwares* semblants en els quals quan tu demanes fer una cosa complicada, és a dir que fas servir un coneixement avançat de l'empresa, l'empresa no et dona el *software* perquè t'ho faci, sinó que et demanen accés remot al telèfon, per exemple, perquè ells executin coses i tu no saps el que executen i et donen el resultat. És a dir, prenen mesures per tal de que el seu coneixement no surti de l'empresa.

Llavors, podem esperar que si hi ha alguna instal·lació probablement hi ha un control d'aquest tipus, però no sabem si és només el *software* o també les dades, això no ho coneixem.

Hi havia alguna cosa més? Més o menys contestem? *(Veus de fons.)* Sí, sí. I sobre el nombre d'infectats, no ho sé, o sigui, nosaltres hem fet el nostre... Abans preguntaven sobre el nombre. Estem parlant..., nosaltres hem analitzat desenes de mòbils. Evidentment, no és comparable als milers que va reportar WhatsApp. WhatsApp, el que va reportar és ús no autoritzat de la seva plataforma, però no sabem si els 1.400 que van utilitzar aquesta vulnerabilitat de WhatsApp si finalment van ser infectats. Això no ho sabem, però evidentment els nombres de WhatsApp són a nivell global i els nostres són a nivell local.

El president

Moltes gràcies. *(José Navarro Hernández demana per parlar.)* Sí?

José Navarro Hernández

Bé, comentaven des de quan està actiu. Nosaltres, dels informes de Citizen Lab, sabem que NSO comença a caminar l'any 2010 i poc després ja comencen els primers informes de Citizen Lab. La nostra anàlisi és més moderna, perquè entenc que l'espionatge al nostre entorn es va fer després i també perquè els rastres es van perdent amb el temps i nosaltres vam fer les anàlisis fa relativament poc. O sigui, nosaltres podem parlar –parlo de memòria– del 2017, una cosa així, no?, 2018 en endavant. Sí, més o menys coses així, fins al 2020-21.

El president

Gràcies, senyor Navarro. Senyora González.

Jessica González Herrera

Sí; gràcies, gràcies, president. I gràcies al senyor Navarro per la seva compareixença. Jo mateixa no soc la diputada adscrita a aquesta comissió d'investigació; és el diputat Lucas Ferro, que recuperarà la intervenció.

En tot cas, aspectes que ja s'han tocat per part dels altres grups parlamentaris. Per nosaltres és important que es pugui depurar, saber exactament què va passar, on estan els forats de seguretat i agraïm la vostra compareixença en aquest sentit perquè, en aquest cas, i tenint en compte la naturalesa també de la investigació, no només cal una investigació judicial, sinó també política.

Afegint a tot el que s'ha fet l'única pregunta que li plantejaríem i, si de cas, el diputat ja s'adreçarà a vostè si hi ha qüestions a ampliar més en detall –i té a veure amb el que ens competeix en aquesta casa, no?, en el Parlament de Catalunya–, si és que heu fet alguna valoració de que el marc legislatiu que tenim actualment pot ajudar, pot millorar, pot contribuir d'alguna manera a la vostra feina, i protegir encara més i que no es tornin a repetir casos com aquests, en clau parlamentària i específicament, si creu que hi ha alguna modificació o algun marge de millora que tinguem per tal d'anar un pas més enllà i protegir la seguretat sabent que tot això està fora de la legalitat, en el sentit de que hi ha invasions de la privacitat, però si en el marc del que podem fer és des d'aquest Parlament pel que fa a legislació, considereu que alguna modificació o alguna legislació que no existeix, tenint en compte també com avança tot el tema de les tecnologies, podria contribuir a les garanties de no repetició d'un fet tan greu com aquest.

Moltes gràcies.

José Navarro Hernández

A veure, jo insisteixo que nosaltres som tècnics, som informàtics i, des del punt de vista de dret no podem opinar. No podem valorar si això és legal, no és legal, això no és la nostra feina. Jo només aconsellaria, i és un nivell de consell, equiparar la intervenció de dispositius amb Pegasus, amb la intervenció de dispositius amb altres sistemes que sí que són legals i estan recollits als procediments legals habituals.

O sigui, hi ha procediments escrits per fer tuteles judicials d'aquest tipus d'intervencions; hi ha procediments molt concrets per com s'han de guardar, com s'han de comunicar, etcètera. I hem de recordar que intervencions digitals, les que coneixem actualment, poden enregistrar d'un telèfon mòbil d'una persona on navega, on és, localització, qui truca, agafar continguts de trucades, etcètera. O sigui que Pegasus evidentment és un sistema molt més avançat. Pot envair molt més drets fonamentals, evidentment, però jo no puc valorar si és il·legal o no. El que sí que puc dir és que hi ha altres coses que també envaeixen drets fonamentals i que, entre cometes, són legals.

Llavors, jo aconsellaria intentar fer comparació. Coneixem el cas, agafem el que coneixem, agafem Pegasus i anem a veure si s'ha fet com s'hauria d'haver fet amb altres sistemes. Coneixem el proveïdor? Coneixem d'on està tutelat? Hi ha hagut autorització judicial? S'ha respectat la forma? Etcètera.

El president

Moltes gràcies. Senyor Martín Blanco.

Ignacio Martín Blanco

Gracias, presidente. Señor Navarro, en primer lugar, buenos días. Gracias por su comparecencia. La verdad es que el tiempo apremia. Le pediré un poco de lenidad, como siempre, presidente, pero en todo caso intentaré no excederme demasiado de los cinco minutos previstos.

La verdad, señor Navarro, es que debo empezar esta intervención reconociéndole a usted que es usted el experto y, por tanto los demás, los que estamos aquí, somos legos en la materia y estamos en sus manos. Sí que le pediría, en este sentido, un plus de rigor y un plus de honestidad en sus respuestas, que se le suponen. Pero en todo caso, se lo pido de antemano, porque creo que este tema es un tema esencialmente político.

Aquí hay una serie de grupos que consideran que aquí ha habido una persecución política a un determinado grupo político, en este caso al mundo, al movimiento separatista, y otros que consideramos que esto es un enorme montaje, una causa falaz que lo que pretende es intentar presentar a España como un estado antidemocrático que espía a algunos de sus ciudadanos por sus ideas políticas.

Bien, partiendo de esta premisa, esta dicotomía –algunos grupos piensan eso y nosotros pensamos todo lo contrario–, ya le digo que a mí me parece que el informe de Citizen Lab queda desvirtuado en la medida en que su autor material, el señor Elies Campo, pues, ha demostrado, digamos, una falta de credibilidad importante cuando se ha sabido que ha mentido sobre su currículum, ha dicho que era ingeniero cuando no era ingeniero, ha dicho que ha trabajado para Telegram cuando Telegram niega que haya trabajado para ellos. Por tanto, la propia autoría para mí está desvirtuada de origen.

Pero, insisto, me gustaría conocer algunos detalles que usted seguro que nos puede esclarecer. En primer lugar, me gustaría saber si usted ha trabajado para Citizen Lab o ha trabajado para alguno de los partidos aquí presentes, alguno de los partidos separatistas le han contratado en alguna ocasión para hacer algún informe, alguna averiguación con relación al asunto de Pegasus. Me gustaría saber si usted o alguno de sus compañeros estuvo implicado en los análisis que tuvieron lugar en el año 2020 –para nosotros es importante–, que son los que supuestamente acreditan esa infección, que, digamos, algunos arrojan dudas sobre si realmente es una infección en el momento en el que se dice o es una infección *a posteriori*.

Me gustaría saber si considera usted importante la cadena de custodia en los análisis forenses y que se documente el proceso de manipulación, como recomiendan ENISA y el protocolo Berkley. Me gustaría saber por qué cree que tanto Citizen Lab como las presuntas víctimas se niegan a que sus teléfonos sean analizados por peritos designados por un juzgado o por expertos independientes. Para mí, eso es muy importante. Me gustaría que me lo contestase, porque creo que es una cuestión que va a la raíz del problema.

¿Por qué cree que Citizen Lab se niega a comunicar cuántos teléfonos fueron analizados o la ratio entre infecciones y análisis? Hablando de la metodología Citizen Lab, usted ha dicho que podía ser criticable en términos técnicos, que no era el espacio, pero esta pregunta me parece pertinente.

Después, Citizen Lab se niega a compartir información sobre cuándo fueron analizados los dispositivos. Por testimonios sabemos que algunos lo fueron en 2020 y otros en 2022. ¿Por qué recomiendan los protocolos de análisis digital forense que se documenten bien, cuándo y dónde y cómo se analizan los dispositivos? ¿Por qué cree que Citizen Lab oculta esta importante información? ¿Por qué la literatura académica sobre análisis digitales forenses recomienda analizar también físicamente los dispositivos? ¿Por qué motivo Citizen Lab no ha realizado ningún análisis físico de los dispositivos?

Si los indicadores de compromiso que usan Amnistía y Citizen Lab para atribuir ataques con Pegasus son públicos, otro *malware* podría imitarlos. El internacionalmente reconocido criptógrafo Nadim Kobeissi ha declarado públicamente: «No solo es muy fácil, sino muy rentable, que existan programas maliciosos que adopten intencionalmente los patrones de comportamiento de Pegasus». ¿Significa esto que personas con alta competencia técnica podrían plantar falsos positivos de Pegasus si les interesase? Esta pregunta para mí es crucial. Me parece muy importante.

Después me gustaría saber si le parece normal que en el llamado informe «Catalangate» se mezclen personas infectadas con personas que solo habrían recibido un SMS sospechoso, pero sin constancia alguna de infección, con personas de las cuales no se tiene ninguna constancia forense de haber sido atacadas, como es el caso de Maragall, Miquel, Domingo y Gabriel.

De ahí, que el señor Gregorio Martín, en su intervención el otro día en el Parlamento Europeo, el señor Gregorio Martín Quetglas dijera que después de examinar la metodología de datos y creando una prueba de concepto que fácilmente falsifica la evidencia presentada, se ha llegado a la conclusión de que no hay pruebas que demuestren que el Gobierno español utilizó el *software* espía Pegasus. El señor Gregorio Martín Quetglas acaba definiendo el documento de Citizen Lab como un documento falaz.

Por tanto, a mí me parece muy importante que, cuando hay expertos reconocidos en la materia que dicen que es fácil crear positivos, usted nos diga su opinión como perito independiente, si realmente eso es cierto, es fácil crear esos falsos positivos. Me gustaría que nos dijese cómo puede usted asegurar que no han plantado los indicadores de compromiso en los meses posteriores al conocimiento público del escándalo, del llamado «Catalangate». Y cómo puede usted saber distinguir si el ataque tuvo éxito o fue simplemente un intento como los muchos que recibimos todos.

Después hay una pregunta que me parece también importante, que es si usted puede detectar las fechas con indicadores de fiabilidad. Si eso es así, si usted puede indicar las fechas, puede saberlo, ¿cómo es que Citizen Lab no? Porque Citizen Lab dice que no las puede certificar.

Y en última instancia, nos gustaría saber, en definitiva, si usted cree que un país como Rusia, un país con la potencia de Rusia, podría llegar a implantar ese tipo de programas espía, si se les requiriese para ello, con lo cual aquí llegaríamos a la clave de la cuestión, de lo que algunos consideramos este documento falaz del que hablaba el señor Gregorio Martín y efectivamente creemos que esto es una burda invención de los partidos nacionalistas para tratar de desacreditar a España, a lo que ellos llaman el Estado español, ante la comunidad internacional.

Pero, insisto, podría ser que nosotros estuviéramos equivocados. Creo que este tema, en todo caso, como han dicho algunos de los compañeros en sentido radicalmente contrario al mío, no es un tema en absoluto claro. Entre otras cosas, porque la mayoría de la población desconoce detalles importantes de la materia de que se trata, la materia informática de la que usted es experto.

Y, por tanto, si me pudiera arrojar luz sobre estas numerosas preguntas que le he formulado, yo se lo agradecería mucho y creo que la opinión pública catalana y del conjunto de España también, modestamente.

Gracias, señor Navarro. Gracias, presidente, por su lenidad. Gracias.

El president

Moltes gràcies, senyor Martín Blanco. Senyor Navarro.

José Navarro Hernández

Gracias. A ver, nosotros actuamos..., ya lo he comentado antes, nosotros actuamos como peritos. Entonces, como peritos en procesos judiciales, nosotros lo que solemos hacer es aportar resultados técnicos. Lo que luego el juez haga con esos resultados técnicos a la hora de valorar su sentencia, eso ya no es cosa nuestra. Es decir, yo le puedo decir lo que hay a nivel técnico. Si esto demuestra x o desmiente y, esto yo ya no lo puedo decir.

Lo de categorizar como «falaz» el informe Citizen Lab –y empiezo por ahí porque tiene implicaciones técnicas importantes–, a mí no me parece adecuado. No me parece adecuado no por las palabras, sino por cómo se motiva en la propia intervención del señor Martín en el Parlamento Europeo. Es decir, en su intervención y en lo que ha escrito, que le he seguido un poco, no hay argumentos técnicos importantes.

Por ejemplo, comentaba: «Es criticable mezclar en el informe "Catalangate" personas cuyos teléfonos estaban infectados con las que no». Esto, para mí eso..., para mí lo importante de sus informes es que incluyen evidencias de los que sí están infectados. Si se ponen...

Ahora no recuerdo en qué contexto salían, por ejemplo, nombres de personas cuyos teléfonos no estaban infectados. Pero si se ponen, para poner encima de la mesa el muestreo estadístico que se ha hecho, para que se tenga una idea de que «oiga, no solo hemos analizado y encontrado positivos, sino que también hemos encontrado negativos», a mí me parece bien. Porque, al final, si tú estás haciendo análisis de teléfonos y todos te salen positivos sería sospechoso.

En cuanto a la metodología de Citizen Lab, ya lo he explicado un poco, no lo repetiré –si tiene alguna pregunta concreta, se la puedo responder–, pero para mí, a grandes rasgos, lo que es criticable de la metodología de Citizen Lab no es el desarrollo técnico que hacen ni el desarrollo de implicación lógica a lo que concluyen a partir de resultados técnicos, sino que ahora, en el año 2023, el ir a reproducir los resultados no es posible, pero no porque ellos hayan hecho algo mal, sino porque yo ahora no puedo escanear el internet que había en el año 2015.

Ellos, en el 2015, hacen unos escaneos de internet para identificar qué patrón tienen esos servidores de NSO y yo, evidentemente, hoy en el año 2023 no lo puedo hacer. El que ellos no hayan hecho una cadena de custodia de esa información entonces, esto es lo criticable. Pero claro, dices, ¿esto tira todo el informe? No, primero porque ellos en su día no actuaban como peritos sino como investigadores. Por lo tanto, no tenían ese requerimiento acerca de la custodia que, por cierto, está como requisito en el nuevo Código penal. Hay un apartado en que dice que cuando se aportan pruebas, se deben aportar con los mecanismos que aseguren... Sobre el tema de la cadena de custodia, creo que era una pregunta que hacía, es importante. Pero, dos, pero no es crítico. Hay jurisprudencia y hay muchas.... Es que hemos ido a muchas charlas de magistrados y demás, y esto es una pregunta recurrente que hacemos: Cuando la cadena de custodia está mal hecha o no existe, ¿esto invalida la prueba? Y la versión unívoca de todos los jueces –y perdone que hable de jueces, pero es lo que conozco, ya sé que no es extrapolable a lo que hay aquí, pero– es que no. Es decir, el juez valorará. Y hay muchas sentencias donde no hay una cadena de custodia. Se quejan por esto, pero el juez dice: «A mí..., yo es que esto..., no me creo que aquí haya una manipulación.»

Tercero: si hay manipulaciones, muchas veces se puede ver en un análisis forense posterior. Nosotros, en muchos casos, hemos encontrado, pues, que tú vas a hacer un análisis forense, te trae un cliente un ordenador, te dice: «Oye, mira, porque creo que este comercial está accediendo a información de la competencia, está accediendo a información de...», y ves que la información te la ha puesto el cliente para crear prueba falsa. Hemos tenido algún caso de estos, es decir, nosotros normalmente hacemos análisis para intentar ver si las pruebas que estamos obteniendo han sido manipuladas o no. Y hay diferentes técnicas para hacer esto.

Lo importante al hacer una cadena de custodia es que yo las haré y yo le puedo decir que, de los resultados de mi informe, podemos concluir que los resultados son confiables, es decir, confiamos en que realmente ha habido una infección en la gran mayoría de estos teléfonos. Pero lo bueno es que nosotros sí que hemos hecho una cadena de custodia; es decir, si otra parte no está de acuerdo, puede rehacer el análisis o hacer un análisis diferente y probar que hay una manipulación.

Si tuviéramos un solo teléfono sería débil, porque a lo mejor un solo teléfono con dos indicadores igual has encontrado una manera de manipularlos sin crear rastro. Pero tenemos muchos teléfonos. Entonces, el poder manipular todos estos teléfonos de personas diferentes, en realidades sociales diferentes, de organizaciones diferentes, de la misma manera, de manera que no creen un registro o un indicio de que hayan sido manipulados, yo lo considero, no voy a decir imposible, porque yo soy

científico, no lo voy a decir, pero es altamente improbable. Es decir, se puede confiar que no ha habido una manipulación de datos, al menos en los teléfonos que nosotros hemos analizado. Y podemos tener confianza de que los registros que nosotros vemos indican un acceso no autorizado con un *software* malicioso que intenta ocultarse y que transmite datos a internet.

Esto es lo que podemos dar confianza. En lo que se interprete políticamente de esto, yo ni entro ni quiero entrar. Me preguntaba: «¿Nos puedo decir quiénes son sus clientes a nivel político?» Al principio de todo de mi brevísima intervención, le he dicho que es una de las cosas que no puedo decir, pero le introduzco que, a lo largo de todos estos años, si no hemos trabajado para todos los partidos políticos, pocos habrá que queden. Es decir, somos un despacho pequeñito, no estamos politizados. Es decir, no tenemos ese problema.

No qué me quedaba más. *(Veus de fons.)* Sí, sobre que Citizen Lab oculta información o que su metodología no es corre... Es que el trabajo de Citizen Lab, tanto el de Citizen Lab como el de Amnistía Internacional, desde mi punto de vista, es un trabajo científico. Si ustedes están acostumbrados a leer trabajos científicos, son trabajos científicos que se deben atacar desde el punto de vista científico. ¿Que no estás de acuerdo? Perfecto. Hay cosas que son atacables. Pues, escribe un artículo científico, haz un análisis, publícalo.

Yo, ya le digo, las críticas que he escuchado, que no solo ha sido la de Gregorio Martín, yo no he escuchado ninguna crítica concreta, objetiva, técnica, y a mí me interesaba, porque nosotros nos basamos mucho en la metodología de Citizen Lab, así como la Amnistía Internacional –no es la única, también hacemos nuestros análisis, es decir, tenemos estas tres patas, pero evidentemente lo histórico que ha hecho Citizen Lab es muy importante–, y yo no he encontrado ninguna crítica técnica objetiva que pueda ser aplicada, por ejemplo, a las cadenas de custodia que tenemos nosotros para poder demostrar que esos resultados son falsos.

Y, por último, ya sé que me paso del tiempo, pero es importante. muy brevemente le diré que, porque preguntaba también, sobre las cadenas de custodia, se pueden contraanalizar, es decir, un perito ahora puede venir. Creo que no palos en las ruedas a esto. Lo que pasa es que hoy en día no está resuelto, y creo que lo comentábamos también en un podcast nuestro, es información pública, hoy en día no está resuelto cómo se debe acceder a la cadena de custodia hecho por otro perito para hacer una contrapericial. Sobre todo, en casos de teléfonos móviles, esto es muy reciente. Antes, cuando tenías un ordenador corporativo, por ejemplo –nosotros hemos hecho muchas contrapericiales–, donde el otro perito ha hecho una cadena de custodia, ha hecho su análisis, yo voy, le copio el mismo ordenador y hago mi contraanálisis. Nunca ha habido problema con esto.

Cuando entramos en el terreno de teléfonos móviles hay un problema, porque con un ordenador corporativo hay una clara división entre el contenido personal y corporativo, pero en un teléfono no. Entonces la invasión de derechos fundamentales hay que cogerla con pinzas aquí. Y el derecho de una persona a aportar prueba, que es un derecho fundamental, entra en colisión con su derecho fundamental a la intimidad y secreto de comunicaciones. Entonces es algo que no está muy resuelto.

Entonces, el *mosso d'esquadra*, la policía judicial o el perito privado que vaya a hacer una contrapericial de lo que nosotros hemos custodiado, ¿debe tener acceso a todo el teléfono? Técnicamente, yo diría que sí, porque es la única manera de utilizar las mismas armas. ¿Tiene el propietario del teléfono derecho a que se controle este acceso para que él tenga garantías de que no se accede a nada que no sea relevante para el caso y que no pueda extraer información de manera no controlada? También. Entonces, ¿cómo se juntan estas? Nosotros tenemos, porque hemos hecho cosas así.

Por ejemplo, nosotros hemos hecho muchas contrapericiales, con el perito del otro lado o con el abogado el otro lado aquí, o con un notario aquí o en la misma

sala del juzgado. Entonces, hay maneras de hacerlo, pero hay que controlarlas, evidentemente, hay que respetar los derechos de todas las personas.

El president

Moltes gràcies, senyor Navarro. Moltes gràcies per les seves respostes, les seves exposicions. Si ara els sembla bé i a tots els grups els sembla bé, faríem la segona compareixença, del senyor Elies Campo, que... Sí? *(Ignacio Martín Blanco intervé sense fer ús del micròfon.)* Obriríem un torn a tots els grups, eh? *(Ignacio Martín Blanco intervé sense fer ús del micròfon.)* D'acord.

Ignacio Martín Blanco

Gràcies, president. Senyor Navarro, gràcies per les seves explicacions, esclaridores, sens dubte. M'ha quedat com, en la seva condició d'expert, m'ha quedat una mica pendent saber per què creu vostè que els afectats es neguen a un informe fet per les autoritats judicials o per experts independents? Deia vostè el tema de la protecció de les dades, per descomptat, això és fonamental, la protecció dels drets fonamentals.

Ara, jo crec que això és una qüestió clau. És a dir, si estem parlant d'un gran cas, un escàndol, d'una persecució política com alguns sostenen aquí i alguns diem que és tot el contrari, que segurament és o tenim la impressió que pot ser una causa inventada, una altra fal·làcia del món independentista, doncs, el que considerem que seria bàsic és que hi hagués experts independents o experts judicials que fessin aquesta comprovació.

A mi m'interessaria molt conèixer la seva opinió com a expert. I després no sé si això ens ho pot dir o no, però saber del cert si vostè o algun dels seus companys va participar en l'anàlisi dels terminals implicats que van tenir lloc el 2020. Perquè això sí que és important, perquè hem sabut que alguns han reconegut que no havien estat infectats inicialment però que després van sortir infectats en aquesta anàlisi del 2020. I em semblaria interessant saber-ho.

Gràcies, senyor Navarro. Gràcies, president.

El president

Moltes gràcies, senyor Martín Blanco. Miri, aprofitant que avui hem après moltíssimes coses sobre peritatges i sobre infiltracions o temes informàtics, i jo fins i tot he aprés una paraula que no coneixia, que era la «*lenidad*», que vostè m'ha dit, cosa que és clar, la definició me deixa una miqueta preocupat, però bé, eh?, li respecto, i també si a vostè li sembla bé, el senyor Navarro contestarà si ho troba oportú, a la primera pregunta que ha fet. però si vostè també em permet aquesta *lenidad*, en aquest cas per part seva, i m'ho permeten la resta de grups, jo soc president, però també soc una de les persones que presumptament o jo crec he estat infectada, li contestaré aquesta pregunta que ha fet, perquè crec que per vostè és molt important. I si vostè vol, jo, no com a president, sinó com a, diguem-ho així, ja sé que no és així, però com a testimoni li podré contestar exactament a això que vostè ha preguntat perquè li ha demanat una opinió a un pèrit, fent referència a actuacions que, en aquest cas, per exemple, m'afecten a mi, i ell pot donar la seva opinió sobre el que jo penso, però jo si vol i la resta que us ho permeten, li contestaré.

Senyor Navarro.

José Navarro Hernández

Sí, sobre l'última pregunta, de veritat, me n'havia oblidat. O sigui, quan parla de les anàlisis de 2020, entenc que són les anàlisis que motiven els articles i tal. No, nosaltres vam ser contractats formalment després, tot i que vam ser contactats abans, per veure si podien fer-ho, tal i qual, però no vam fer res abans. O sigui, nosaltres van començar després.

Sobre la primera pregunta, ja li he contestat, o sigui, nosaltres..., el que li puc dir és que fora d'aquest cas, a altres casos de separacions, de contractes, d'àmbit civil,

àmbit social en què els mòbils s'aporten com a mitjà de proves, la gent té les mateixes reticències, és a dir: «Oh, com que copiaràs tot el meu telèfon mòbil? Però qui podrà accedir al meu telèfon mòbil? Ui, ara m'han de fer un contraperitatge, però accedirà a tot el meu telèfon mòbil?» Això passa, o sigui, és un àmbit, és una preocupació intrínseca de l'ésser humà. No és particular d'aquest cas i per això comentava que s'han d'adoptar solucions que encara no estan adoptades. Per això es recomana, en aquest cas, ser molt prudent, en com es fa la contrapericial.

El president

Moltes gràcies, senyor Navarro. Vol que li contesti la seva preocupació? Li interessa? Ho dic perquè ha llençat unes acusacions. Ara no ho faig com a president, eh? Si vol, m'assec allà com a membre del meu grup parlamentari.

Ignacio Martín Blanco

A mi, francament, president, la seva opinió sempre m'interessa. O sigui que...

El president

Moltes gràcies, senyor Martín Blanco. Vostè preguntava per què les suposades víctimes, si vol, les presumptes víctimes no han aportat contraperitatges més enllà dels informes de Citizen Lab o d'Amnistia internacional i per què no deixen que algun cos policial analitzi els seus terminals mòbils. Li respondré molt fàcilment.

No és veritat. El problema que hi ha és que les contrapericials que es puguin aportar o les anàlisis per part de cossos policials, nosaltres, almenys parlo per mi, el que volem és que un jutge ho demani. No les portarem perquè sí. I resulta que quan hem presentat querelles, moltes d'elles no han estat acceptades; algunes han estat encallades i no es fan les diligències que els querellants hem proposat. Però també li avanço: en el meu cas concret, és que em penso que és l'únic tribunal en el qual la jutgessa està actuant per ordres de la sala de l'Audiència de Barcelona, perquè ella s'hi negava, hi hauran contraperitatges. Ja els té el contraperitatge i hi haurà informes de cossos policials sense cap mena de problema.

I a partir d'aquí podrem respondre a les seves preocupacions. Però clar, això depèn també de la col·laboració per part de les fiscalies i dels tribunals, i en aquest cas només ho hem trobat en un cas. I no pateixi, que no tenim res a amagar. És més, com que sabem que les nostres dades personals que explicaven la resta de companys i companyes estan no sabem on, però algú les té, ja no ens ve d'aquí. D'acord? Moltes gràcies.

Fem això. Faríem la següent compareixença. Jo els prego... *(Oscar Aparicio Pedrosa demana per parlar.)* Ah, perdó, perdó, sí, sí, perdó, sí, sí, perdona, senyor Aparicio, endavant.

Oscar Aparicio Pedrosa

Ja que obrim un torn, jo bàsicament dues coses. A veure, ja li dic que li faré arribar per escrit, després és voluntari si vol contestar o no a les preguntes.

Jo ara em vull situar una miqueta. Vostè ha comentat que ningú qüestiona Citizen Lab, com a mínim des de qüestions tècniques. Jo soc advocat i, per tant, jo no puc entrar a determinar qui té raó, però sí que com a advocat el que m'agrada és que hi hagi contradicció i, per tant, nosaltres sabem –ho sabem nosaltres i ho sap tothom– que hi ha com a mínim dos professors que se n'ha citat aquí el nom i un tercer, que és el senyor Jonathan Scott, que han fet informes qüestionant. Per tant, nosaltres sí que el que volíem és que en aquesta comissió es pogués escoltar tothom: vostè, com ho ha fet, vindran representants de Citizen Lab, també ens agradaria escoltar els altres, per poder determinar o poder treure l'entrellat de com ha anat tot això.

En tot cas, jo de la seva..., li havia fet la pregunta sobre les vulnerabilitats de WhatsApp, per què no coincidien, si hi havia altres empreses en tecnologia zero clic, etcètera, que no m'ha contestat, en tot cas ja l'hi faré arribar. Però sí que a mi al final vostè, a preguntes del senyor Nacho Martín Blanco, ha contestat que saben

que hi ha infectats, que hi ha dades infectades, però clar, aquí nosaltres, en aquesta comissió, el que hem de determinar és si s'ha fet amb Pegasus o amb Candiru, però qui ho ha fet. Jo crec que aquesta és la pregunta que, en teoria, hem de contestar en aquesta comissió.

I, per tant, no sé si vostè és capaç, de les anàlisis de les..., perdoni, em sembla que ha dit setze terminals, no ho recordo exactament, eh? M'ho he apuntat, però he posat entre dotze i setze, perquè no he entès si eren dotze o setze, però és igual. De les terminals que vostè ha detectat o ha inspeccionat i que hi ha infecció, si pot determinar qui és el responsable d'aquesta infecció.

Moltes gràcies, senyor president.

El president

Moltes gràcies. Va, doncs fem, si de cas, un torn, i després contesta a tots i així tancarem.

Josep Rius i Alcaraz

És molt ràpid i no és per fer cap pregunta, però només per deixar constància que és sorprenent la voluntat que tenen uns només de mirar de desacreditar, d'amagar i de no voler, diguem-ne, donar cap tipus de veracitat al major escàndol d'espionatge que hi ha hagut al món i que ha estat acreditat d'entrada per un laboratori de la Universitat de Toronto, i la voluntat dels altres grups polítics de voler que s'investigui, de voler portar gent amb una capacitat i una professionalitat fora de tot dubte aquí, per mirar que s'esclareixin els fets que han passat i aquesta responsabilitat.

Jo crec que diu molt ja de l'actitud de determinats grups parlamentaris, diguem-ne, de la voluntat amb la qual estan actuant en aquesta comissió d'investigació.

El president

(Remor de veus.) Sense el «micro» no... No ens esverem. Fem la compareixença i després, si volen, obrim un torn, quan acabin la segona compareixença i fem els debats que vagin més enllà. Senyor Orobitg.

Jordi Orobitg i Solé

Sí; només un breu incís. Abans, quan li he plantejat la pregunta, vostè m'ha dit que existeixen eines tecnològiques ja que venen previstes en el propi Codi penal i que és de domini públic que la seva utilització tant per cossos policials i amb la preceptiva autorització judicial..., i de les seves pròpies paraules jo entenc que Pegasus no forma part d'aquest *software* que habitualment s'ha utilitzat, doncs, en aquest marc reglat convencional i que és de coneixement dels cossos policials i, en aquest cas, de les autoritats judicials que validen la seva utilització.

Per tant, tenint en compte que Pegasus no forma part d'aquestes eines, i entenc que no és una consideració política que li estigui demanant, vull dir, la pròpia admissió explícita per part del Govern espanyol de que s'està utilitzant aquesta feina, fora d'aquest marc regulat, podria comportar que l'autorització judicial que s'ha rebut per la seva utilització hagués estat en desconeixement del jutge que ho va validar de quina era l'eina tecnològica que s'utilitzava? No sé si m'estic explicant.

Vull dir, es pot haver enganyat el propi magistrat que ha autoritzat aquestes divuit escoltes reconegudes pel Ministeri de Defensa espanyol per mediació del Centre Nacional d'Intel·ligència.

I una altra consideració. Quan vostè ha dit que no coneix cap anàlisi científica que invalidi les conclusions dels estudis de Citizen Lab i d'Amnistia Internacional, perquè no fa una aportació tècnica que desacrediti aquelles conclusions, també inclou aquest darrer informe que s'ha esmentat del senyor Michael Scott, Michael, no sé... Perdó? *(Veus de fons.)* Jonathan Scott, que si no ho tinc mal entès, també el van expulsar de la seva universitat, però bé, i té plantejaments bastant trumpistes. I acabaria únicament amb això, si cal incloure dins d'aquest concepte que no inva-

lida les conclusions, doncs, aquesta... si té coneixement d'aquest estudi i si també resulta desacreditat.

Gràcies.

El president

Moltes gràcies. Senyora Vinyets.

Montserrat Vinyets Pagès

Sí; només una pregunta. Vostè ens ha dit que també, per la seva activitat professional, fa peritatges de separacions, divorcis, espionatge industrial... Li pregunto: fer aquest peritatge li ha comportat un plus d'exigència, de dificultat ja que aquest troià es va concebre precisament per no ser descobert i no deixar rastre? Si hi ha unes dificultats afegides en fer peritatges amb relació a aquests programaris.

Gràcies.

El president

Senyor Navarro.

José Navarro Hernández

Sí; començant potser per l'última. Hi ha molts casos en els quals tenim aquest tipus de dificultats. Per exemple, quan una persona esborra coses d'un ordinador i l'empresa ens truca sis mesos després. Llavors les traces que queden a l'ordinador ja no són tan fortes i hem de fer un esforç i potser la pericial després no és tan forta. En aquest cas és que el sistema està dissenyat per ser invisible, tot i que no ho aconsegueix. I per això, i gràcies al treball de Citizen Lab, Amnistia Internacional i altres grups, perquè no són els dos únics, doncs, hem pogut identificar el patró de comportament. O sigui, bé no...

O sigui, hem tingut dificultats addicionals? Sí, però és que en altres tipus de casos més normals ja en tenim. L'únic aquí és que les conclusions no solen ser tan fortes com «trobem un PDF a l'escriptori que diu, sí, "Mi plan para hacer competencia desleal", sí, doncs, l'he trobat, senyoria». Aquí, bé, queda més... Nosaltres intentem limitar lo que són els resultat tècnics del que després es pot interpretar políticament i judicialment. Nosaltres arribem fins a aquella part.

Això lliga una miqueta amb la primera pregunta, la identificació de qui ha instal·lat tot això? Nosaltres..., només avançaré que a la nostra anàlisi podem dir que tenim un grup de telèfons gran, que podem dir que han sigut infectats pel mateix client d'NSO, i que molt probablement la infraestructura estava a territori espanyol. Més enllà d'aquí no podíem dir nosaltres tècnicament re, tot i que d'aquí, si avancen els requeriments judicials que han d'avançar, podria ser que sortís alguna altra dada que després es pugui relacionar amb una organització o alguna empresa que tingui algun tipus de significat.

Però per ara són els resultats que tenim. Jo crec que és difícil saber per aquesta via, una anàlisi tècnica, qui hi ha darrere. Jo crec que hauria de ser –i ja enllaço a la segona, a la segona pregunta– més per l'altra via. És a dir, SITEL, SILC i tal són sistemes tecnològics que nosaltres sabem que s'utilitzen perquè a nosaltres ens arriben pericials i hem de contraperitar. Llavors, contestant, nosaltres no ens hem trobat un contraperitatge fet amb Pegasus, encara, ni amb *software* similar, però sí que, per exemple, hem fet contraperitatges de casos en què s'han fet servir policies encoberts, per exemple.

O sigui, que aquesta nova normativa del Codi penal sí que s'està utilitzant, el que no sabem, perquè som tècnics, és quins requeriments s'han de seguir per validar una eina d'aquest tipus. Ja sap que en aquest cas és més complicat, perquè el CNI, perquè són secrets, perquè bla, bla, bla, però no ho podem dir.

I també li puc dir que el jutge normalment no diu: «Utilitzi l'eina aquesta per fer això.» Els jutges, i de fet ho han de fer així, han de dir: «Vostè faci una intervenció per agafar converses, per agafar...» És a dir, diu el que vol i després l'eina tècnica

que s'utilitza ja és una altra cosa. O sigui, jo entenc que hi ha d'haver una autorització judicial on es digui què és el que s'ha d'intervenir i allà sabrem qui l'ha ordenat, què s'ha intervingut i què es conserva i en quines condicions.

El president

Moltes gràcies, senyor Navarro. Si els sembla fem això, faríem després la compareixença del senyor Elies Campo. Ja els demano, per temes personals, deu minuts i suspenem un moment la comissió deu minuts i d'aquí deu minuts fem la segona part de la comissió. *(José Navarro Hernández intervé sense fer ús del micròfon.)* Sí.

José Navarro Hernández

Molt breu, molt breu. Ho sento, és que s'ha oblidat una menció a l'informe de Jonathan Scott. El coneixem i entra dins de la mateixa categoria, és a dir, no conté cap anàlisi tècnica objectiva que ataqui res. O sigui, si ho tingués, ho comentaria, però com que no ho té, jo prefereixo no opinar. Ja està.

El president

Moltes gràcies. Ara sí, deu minuts, doncs.
Gràcies.

La sessió se suspèn a dos quarts de dotze del migdia i deu minuts i es reprèn a tres quarts de dotze i deu minuts.

El president

Moltes gràcies a tots per reprendre aquesta sessió de la comissió d'investigació.

Compareixença d'Elies Campo, membre de The Citizen Lab, en qualitat de testimoni

365-00010/13

Moltes gràcies al senyor Elies Campo, que és el que farà la següent compareixença que teníem programada per avui, moltes per la seva assistència.

Recordo una mica el funcionament de la comissió, i com que se'ns ha allargat una mica la primera part i per intentar que ens quadrin agendes a tots plegats, el que faríem seria ara una primera intervenció seva, si vostè ho considera oportú, fins als trenta minuts. Llavors donaríem pas a tots els grups parlamentaris, que un rere l'altre farien les preguntes o les consideracions que considerin. Llavors, vostè contesta i si els grups volen un aclariment, faríem després un minut per a cada grup parlamentari per fer aquests aclariments a la seva resposta, d'acord? Doncs molt bé, senyor Elies Campo, ja té la paraula.

Elies Campo (membre de The Citizen Lab)

Moltes gràcies per convidar-me a aquesta sessió. He preparat una presentació bastant curta, que podem anar més o menys ràpid i crec que el més important és anar a les preguntes. Explicaré què és Citizen Lab, com vam trobar Pegasus, com funciona Pegasus, els principals descobriments del *report*, que també us he compartit amb tots per *email*, l'última versió del que tenim. Quan el tinguem en català també us el faré arribar. I, finalment, les conclusions que vam treure del *report*. I si us sembla, podem començar les preguntes.

Citizen Lab és un laboratori de la Universitat de Toronto, que està situat a la Munk School of Global Affairs and Public Policy i basem la nostra recerca en la intersecció de tecnologies de la informació, els drets humans i la seguretat global. El laboratori va començar el 2001, el va fundar el Ron Deibert, el professor Ron Deibert, que és el fundador i director de Citizen Lab des de que el va fundar. I des de que es va fundar Citizen Lab s'han publicat més de cent cinquanta *reports* on s'han trobat diferents tipus d'abusos, d'abús d'aquest tipus de tecnologia de *spyware* o al-

tres abusos de tecnologia relacionats amb privacitat, sempre focalitzada en aquests tipus d'abusos contra la societat civil.

D'aquests *reports* que s'han publicat, mai cap ha estat qüestionat per cap font fiable tecnològica. I el 2000..., a l'agost del 2016, per primer cop, vam documentar que existia un *software* de *spyware* que es deia Pegasus i el vam documentar per primer cop perquè un activista de *Saudi Arabia* que es deia Ahmed Mansoor ens va enviar un SMS que havia rebut i pensava que devia ser alguna cosa sospitosa.

Aleshores, aquell SMS el vam poder utilitzar al laboratori i vam poder fer clic en aquell laboratori i vam poder capturar una infecció de Pegasus en el laboratori. Per primer cop es va documentar i es va comunicar globalment que existia aquest tipus de *software*, que s'estava utilitzant en contra la societat civil i a partir d'aquí hem anat documentant altres casos. I els casos més aviat que hem trobat són indicis el 2015 d'algun SMS que hem trobat, que hem pogut atribuir també a la infraestructura d'NSO en el cas de Mèxic i en el cas català amb el Jordi Sànchez també vam trobar SMSs del 2015.

Les primeres infeccions que s'han documentat són del 2016. Infecció i objectiu és diferent. En una infecció es pot documentar de manera forense que el *software* ha estat en aquell dispositiu; objectiu vol dir que hem trobat indicis, normalment a través d'SMS, on aquella persona, aquella víctima potencial, va rebre un SMS amb un *link* a la infraestructura d'NSO. Això vol dir que aquella persona va ser un objectiu. En alguns casos podem documentar que realment va haver-hi una infecció i altres no. I aleshores fem aquesta distinció d'infecció o objectiu.

Com funciona Pegasus? Pegasus és un *software* que s'instal·la al dispositiu. Un cop instal·lat en el dispositiu, permet accedir a tot el contingut que l'usuari pot utilitzar o té al dispositiu i tots els sensors d'aquell dispositiu. La gran complexitat és com instal·lar aquest *software* en els dispositius i per fer-ho s'han de saltar totes les mesures de seguretat del sistema operatiu, que totes les empreses que fabriquen aquests tipus de *software* dediquen uns esforços i equips a que això sigui el més difícil possible.

Aleshores la gran dificultat és com saltar-se aquestes mesures de seguretat i com salten aquestes mesures de seguretat va variant al llarg del temps perquè les empreses troben o es comuniquen aquestes vulnerabilitats i les empreses que fabriquen i desenvolupen aquest *software* les van corregint; com és el cas de Citizen Lab, en molts dels casos que hem trobat. Normalment abans de publicar comuniquem la vulnerabilitat que s'ha documentat al fabricant i normalment el fabricant envia una actualització que s'envia a tots els dispositius. I la majoria dels dispositius que tenim a les butxaques aquí s'han beneficiat d'aquestes actualitzacions de *software* basades en part de la investigació que hem fet des de Citizen Lab o altres organitzacions similars.

Aleshores la gran complexitat és instal·lar el *software* de Pegasus utilitzant aquestes vulnerabilitats i aquestes van canviant. Per això, un dels esforços d'organitzacions com Citizen Lab o Amnesty Lab és documentar quines són les vulnerabilitats que s'utilitzen, que estan actives i que, per tant, fan els dispositius vulnerables per instal·lar aquest tipus de *software*.

Aleshores, amb això passem a les troballes del «Catalangate». A Citizen Lab hem documentat seixanta-cinc persones que han estat objectius o infectades amb programari espia mercenari, tant Pegasus, globalment entre Pegasus i Candiru, en aquest cas. Seixanta-tres persones van ser objectius o infectades amb Pegasus, quatre amb Candiru i dos van ser objectius o infectades amb els dos tipus de *software*, Candiru i Pegasus.

Les víctimes inclouen membres del Parlament Europeu, presidents catalans, legisladors, juristes, enginyers de *software* i membres d'organitzacions de la societat civil. En alguns casos, hem trobat que també els seus familiars van ser infectats amb aquest tipus de *software*. Vam identificar una vulnerabilitat que no era coneguda an-

teriorment i la vam anomenar Homage. I era una vulnerabilitat d'IOS, de *zero click* i que no havia estat divulgada anteriorment.

Vam veure que aquesta vulnerabilitat no era activa en versions posteriors a la versió IOS 13.2 i, per tant, ja no era una vulnerabilitat que estigués en funcionament o estigués disponible per utilitzar per instal·lar aquest tipus de *software*. No atribuïm d'una manera conclusiva les operacions a una entitat específica, però les proves circumstancials suggereixen una connexió amb una o diverses agències del Govern espanyol. I vam compartir una selecció dels casos amb el laboratori d'Amnistia Internacional, que van validar de manera independent la nostra metodologia.

I les vulnerabilitats que hem trobat amb aquest cas són principalment dos. Un és el que es diu vulnerabilitats de zero clic i l'altre a través de missatges de text maliciosos. En les vulnerabilitats de zero clic, són aquelles vulnerabilitats on l'usuari no ha de fer re perquè se li instal·li el *software*. En el cas de les altres, els missatges de text o *emails*, l'usuari ha de fer una acció, en aquest cas ha de clicar aquell missatge i a partir d'aquell missatge el sistema explota alguna vulnerabilitat en l'explorador d'internet que fa que es pugui instal·lar aquest tipus de programari.

Aleshores les vulnerabilitats de *zero click* són tres són Homage, Kismet i les vulnerabilitats que es van documentar a través de WhatsApp. Tant Homage com Kismet van utilitzar les vulnerabilitats en el sistema de missatgeria d'iMessage d'Apple i permetien rebre un missatge formatat d'una manera especial que feia que es pogués explotar una vulnerabilitat del sistema operatiu i, per tant, instal·lar Pegasus a través d'aquesta vulnerabilitat.

Les vulnerabilitats de WhatsApp també eren *zero click* i aquestes vulnerabilitats les va trobar el propi equip de WhatsApp i va demanar a Citizen Lab que ajudéssim a documentar i a localitzar i a identificar les víctimes d'aquest atac. En el cas de WhatsApp, es va poder documentar de manera forense que havien estat objectius, però no es va poder verificar de manera forense que havien estat infectats a través d'aquesta vulnerabilitat. Això és una de les coses que veig que genera algun dubte.

I els atacs basats en SMSs, normalment són un SMS molt personalitzat a la persona que l'ha de rebre, amb contingut molt personal, relacionat amb la seva vida professional, amb la seva vida personal, amb els viatges, i el contingut d'aquest missatge és generar una resposta impulsiva perquè la persona que rep aquest missatge no pugui ni pensar si ha de fer clic o no en aquest *link* i acabi fent clic en el missatge.

De moment, en aquest cas hem recopilat més de dos-cents missatges d'aquest estil, que varien dels diferents tipus de víctimes. D'alguns d'aquests missatges hem pogut documentar que han sigut satisfactoris a l'hora de poder infectar un dispositiu. D'altres hem pogut documentar que aquest SMS ve i conté un *link* a la infraestructura d'NSO coneguda, però no podem documentar si han estat infectats o no.

Les atribucions de Pegasus NSO, com ha explicat abans el pèrit José Navarro, són a través de diferents metodologies. Una és l'anàlisi exhaustiva de monitoratge a grans escala d'evidències d'infeccions a través de la xarxa, i en el cas d'NSO vam poder documentar que els dominis utilitzats en alguns dels SMSs es corresponien a infraestructura d'NSO de diferents models.

I en les atribucions a Candiru, una metodologia similar, vam poder documentar part d'aquesta xarxa com es comunicava aquest tipus de *software* i el juliol del 2021 es va publicar un *report* que es deia *Hooking Candiru*, on es va documentar que havien treballat amb Microsoft quan vam identificar una infecció activa d'aquest *software*. I en aquell moment no es va anomenar pacient zero, però era un pacient, era una víctima del «Catalangate» que és el Joan Matamala. I aleshores, l'atribució de Candiru en aquest sentit va ser gràcies a poder trobar aquesta..., o una de les raons va ser trobar aquesta infecció activa d'aquest programari en un dispositiu. Quan es troba una infecció activa normalment per a les persones que fan aquest tipus d'in-

vestigació és la manera, una de les principals maneres, que tenim per entendre com funciona aquest programari.

I, aleshores, les diferents conclusions que vam treure són: no podem atribuir-ho directament a un govern, però hi han quatre principals proves circumstancials que apunten a una forta connexió a una o més entitats dins del Govern espanyol, incloent: un, que els objectius eren d'interès evident pel Govern espanyol; dos, que els moments específics dels atacs coincideixen amb esdeveniments d'interès per al Govern espanyol; el contingut dels SMSs d'atac suggereix que hi ha accés a informació personal dels objectius, com números de DNI, el *Passenger Name Record*, que és una numeració que hi tenen accés els governs, i quart, que s'ha informat i documentat públicament que almenys el CNI és propietari i té llicències d'utilitzar aquest programari.

Les conclusions. També fem una crida a una investigació i que la gravetat i l'extensió del cas justifiquen una indagació oficial per trobar o determinar la part responsable. I les preguntes que ens fem són: com es van autoritzar les intervencions; quin marc legal regien aquestes intervencions; quina supervisió judicial s'aplicava; quin és l'abast real de l'operació; els usos als quals es va destinar el material que es va aconseguir; com s'han gestionat aquestes dades, i a qui s'ha pogut proporcionar.

Cal també mencionar que el cas del «Catalangate» és el més extens que hem documentat a nivell de víctimes, però també el més extens de duració temporal. Hem documentat que des del 2015 fins al 2020 s'ha estat utilitzant aquest tipus de programaris.

I si us sembla, no m'estenc més i podem passar directament a les preguntes.

El president

Moltes gràcies, senyor Campo. Doncs ara passaríem així a les preguntes com comentava al començament. Faríem el torn seguit de tots els grups parlamentaris, cinc minuts per cada grup parlamentari. I després el senyor Campo faria les seves respostes i apreciacions.

El senyor Nacho Martín Blanco m'ha demanat si podia ser el primer, perquè havia de marxar, tenia una cita fora i, per tant, comenci vostè, senyor Martín Blanco.

Ignacio Martín Blanco

Gràcies, president. Sí, efectivamente, tengo que salir. La verdad es que el señor Campo ha ido rápido y, por tanto, seguramente, pues, me dará un poco más de tiempo. Pero en todo caso, señor Campo, gracias por su intervención. Repito lo que le he comentado al señor Navarro. Aquí hay varios grupos que parten de una premisa, que es que aquí ha habido un caso de persecución masiva a un movimiento político por razones ideológicas. Y eso se pretende imponer en la opinión pública como una verdad irrefutable.

Yo, mi grupo, una parte de la sociedad catalana y del conjunto de la española, partimos de la opinión radicalmente contraria, que es que aquí hay una operación orquestada por los partidos nacionalistas, por los partidos separatistas, para tratar de degradar la imagen internacional de España y presentar España como un estado antidemocrático que persigue a quienes se han declarado objetivamente como enemigos de la propia unidad del país.

Paso a las preguntas, señor Campo, porque el tiempo es limitado. En 2020, Citizen Lab estaba trabajando para WhatsApp esclareciendo si los afectados por la brecha de seguridad habían sido espiados, ¿correcto? ¿Cómo descubrió Citizen Lab que había 1.400 personas espiadas en todo el mundo? ¿Qué *software* utilizaron para confeccionar la lista?

Cuando usted contactó por primera vez a Citizen Lab en julio 2020, se presentaba como directivo de Telegram y ha declarado en varias ocasiones que contactó con antiguos compañeros de WhatsApp para verificar si los espionajes, los supues-

tos espionajes, al señor Roger Torrent y otros líderes eren creíbles. ¿No le parece que estaba incurriendo en un conflicto intereses con estos contactos con WhatsApp? Si usted trabajaba de directivo de Telegram, ¿puede explicarnos por qué esta empresa ha rechazado en al menos dos ocasiones que usted haya estado en plantilla o recibido remuneración alguna de ellos? No deja de resultar un poco llamativo.

¿Puede explicarnos qué experiencia tenía usted en análisis digital forense antes del verano de 2020? ¿Había trabajado en algún proyecto de investigación académica antes? ¿Por qué cree que le confió Citizen Lab a usted la coordinación del trabajo de campo? ¿Conocía usted a alguien en Citizen Lab? ¿Cómo se le ocurrió contactar con ellos?

Según el propio Roger Torrent, en el verano de 2020, usted y el señor Scott-Railton estaban trabajando ya en el informe final, junto a una empresa de comunicación americana. ¿Podría decirnos de qué empresa se trataba y por qué necesitaban una empresa de comunicación o relaciones públicas para un simple informe supuestamente académico? Si estaban ya trabajando en el informe final en el verano de 2020, ¿por qué este no se publicó hasta abril de 2022?

Después, también a este respecto, me interesaría conocer cuándo contactan ustedes con el señor Navarro, si nos pudiera precisar esta cuestión. Usted ha descrito en más de una ocasión cómo explicó al señor Matamala cómo aislar su ordenador para que no pudiese ser espiado. El señor Matamala, al parecer, estaba siendo investigado con una orden judicial. ¿No tiene miedo de que lo acusen de obstrucción a la justicia?

¿Por qué contactó usted en 2022 a muchos líderes independentistas, como el señor Jordi Sànchez, cuyo teléfono había sido analizado sin haberse encontrado infección alguna muchos meses antes, y les pidió que se analizasen de nuevo sus teléfonos? ¿Como es que en 2022 encontraron infecciones de 2017 o 2019 en teléfonos que habían sido analizados ya con resultados negativos? Es decir, no había infección en 2017 y 2019 y, sin embargo, sí en 2022. Eso arroja dudas sobre la trazabilidad de la supuesta infección.

El 27 de julio de 2020 Citizen Lab comunicó a Esquerra Republicana de Catalunya que ninguno de los teléfonos que habían analizado estaban infectados. Torrent, el señor Torrent, ya sabía desde el 16 de julio que no estaba infectado, lo reconoce él mismo en un libro. Me gustaría saber cómo valora usted esa supuesta infección *a posteriori*. ¿Por qué incluyeron en la lista de sesenta y cinco a Maragall, Miquel, Domingo y Gabriel, a pesar de que el análisis forense a su teléfono no dio positivo?

Como usted sabrá, la entonces directora de comunicación de WhatsApp afirmó que no se podía confirmar ninguna infección simplemente por el hecho de figurar en la lista de WhatsApp. Hasta ahora, Citizen Lab ha trabajado para que WhatsApp y Apple pudieran llevar a juicio a NSO. ¿Está Citizen Lab ahora trabando con Google o alguna otra gran corporación para llevar a juicio de nuevo a la empresa israelí o alguna otra? ¿Por qué cree que los servicios de inteligencia le espiarían a usted, como se ha conocido, y a sus padres sabiendo lo costosas que son infecciones con Pegasus? ¿Qué méritos tiene usted para que le hayan sometido a esta supuesta investigación?

¿Cuál fue –y esto es importante, señor Campo, le pediría que contestase especialmente a esta y alguna de las otras preguntas– su participación en el equipo técnico de la plataforma Tsunami Democràtic? Su compañero Jordi Baylina defendió públicamente la utilización de la tecnología *blockchain* como la que aplicaron en la plataforma Tsunami Democràtic para conseguir lo que llaman una democracia líquida y así evitar el control por parte de las autoridades. ¿No les da miedo, señor Campo, que en un sistema así sea muy difícil recolectar impuestos, implementar políticas públicas y se dificultara el control de actividades delictivas como el terro-

rismo, crimen organizado y evasión de impuestos? ¿Por qué Citizen Lab lo contrató en febrero de 2022 y no en 2020, cuando usted empezó a trabajar con ellos?

En fin, señor Campo, su investigación –y con esto acabaría, señor presidente, gracias por su paciencia y su comprensión– su investigación, señor Campo, partiendo incluso desde las bases de la misma y de su propia singladura cuando hemos conocido detalles sobre la idea de que usted se presentaba como ingeniero y después resultó que no es ingeniero, la idea de que usted se presentaba como un antiguo empleado de Telegram que luego la propia empresa lo ha negado, pues ofrece algunas dudas, señor Campo, su propia trayectoria y su propia investigación. Y le pediría que aclarase una buena parte, al menos, de estas preguntas que le he hecho, porque sería yo creo interesante para el conjunto de la opinión pública catalana y la del resto de España.

Gracias, señor Campo. Gracias, presidente.

El president

Gràcies, senyor Martín Blanco. Senyor Aparicio.

Oscar Aparicio Pedrosa

Bé, gràcies, i gràcies per comparèixer. Bé, jo abans no ho he dit, però també gràcies al senyor Navarro, anterior compareixent, que he anat tan directe que no li he donat les gràcies per la seva compareixença.

Avui, per exemple, ens ha... I ho dic per començar, no? Nosaltres... Bé, començaré, perquè a vegades sempre salto, vaig a les preguntes i no faig la introducció. Nosaltres, i ho deixo perquè algú m'ha acusat així, no tenim clar si l'informe de Citizen Lab és correcte o no és correcte. El que sí que tenim clar és que hi ha certes incorreccions, en tot cas, que hi ha... Ho dic, perquè vostès mateixos han anat modificant l'informe, perquè hi ha d'altres persones que són crítics amb l'informe i, per tant, la nostra visió sí que és d'escoltar tothom i en funció d'això, mirar a veure què se'n pot treure, si en podem treure l'entrellat. Li dic, per exemple, això del seu informe i em centraré en el seu.

Vostè avui ens ha passat un nou informe, que m'agradaria saber de quina data és aquesta modificació –no me l'he pogut llegir, perquè l'he rebut al matí– i quines modificacions hi ha hagut respecte als anteriors. Quan li deia que, per nosaltres, aquest informe, doncs, és un de més..., i no s'ho agafi malament, però és així, és un de més que té certes, al nostre entendre, qüestions que s'haurien de dilucidar.

L'hi dic perquè, per exemple..., i posaré uns exemples. En els darrers dies, en diferents entrevistes que han fet persones que han estat presumptament espiades amb el Pegasus, etcètera, estan fent referència a que hi ha o que ells tenen positius que no sortien amb Citizen Lab. Per tant, això, en el nostre entendre, ja demostra que alguna cosa hi ha que es pot investigar o es pot mirar.

Si llegim, doncs, la senyora Elisenda Paluzie i la senyora Míriam Nogueras parlen d'infeccions que li venen prèvies a les que vostès determinen en el seu informe. Em sembla que també la senyora Diana Riba, però això no ho acabo de tenir confirmat. Després, al seu informe, a mi, com li he dit abans, que vostè estava a la sala i per tant ho ha escoltat, jo soc advocat, no soc expert tecnològic, però sí que em sobta la indeterminació que s'aplica a l'informe Citizen Lab, indeterminació que..., per exemple, si no ho recordo malament, ara ho estava buscant, però no ho he trobat, em sembla que hi ha cinc persones presumptament afectades que no hi ha nom de qui són.

O, per exemple, es va modificar amb una d'aquestes versions que l'AC, que sempre s'ha dit que era Antoni Comín, no era Antoni Comín. Per tant, ens agradaria saber qui és aquesta persona. O, per exemple, moltes de les infeccions que vostès diuen estan de forma genèrica. És a dir, hi ha hagut una infecció, però no saben ni la data ni com va estar, que potser és normal, no ho sé, però, clar, això a qui el llegeix, doncs, li genera dubtes.

Em genera més dubtes ara quan l'he escoltat a vostè i, per tant, com que vostè ha escoltat també el senyor Navarro, el senyor Navarro ha dit que han arribat a conclusions similars però no idèntiques a les que fa Citizen Lab. Aquí, en el debat anterior també han sortit, com ha escoltat, diferents informes internacionals o nacionals de gent que qüestiona i, per tant, m'agradaria saber la seva opinió sobre aquest qüestionament que reben per part d'altres persones.

Li dic que m'ha sobtat una miqueta, perquè vostè sempre parla d'una quantitat. Quan dic vostè, perdoni, no li poso de vostè, és el col·lectiu Citizen Lab, una quantitat. A mi, per exemple, com es determina l'univers d'aquestes persones també és una qüestió que m'agradaria saber, perquè tots els membres d'aquesta comissió vam estar a Madrid. La senyora Sophie in 't Veld va dir que Citizen Lab havia estudiat quaranta mil o cinquanta mil telèfons i també que hi havien trobat de tot.

A mi m'agradaria saber aquest univers com el van detectar, sobretot en aquest cas en el cas de Catalunya, perquè, pel que s'ha publicat, vostè o persones del grup de Citizen Lab anaven a buscar o oferien els seus serveis a les persones i, per tant, això m'agradaria saber com ho van fer, com van determinar l'univers. I també si és veritat que hi havia molts més telèfons que investigats que no surten en el seu informe. I si de veritat, com deia la senyora Sophie in 't Veld, que entenc que ha parlat amb vostès, doncs, s'havien analitzat telèfons de persones no independentistes. M'agradaria això que ens ho pogués confirmar o no.

Llavors ja li dic vostè ha vist o ha escoltat o suposo que ha llegit aquests informes que qüestionen l'eina de detecció que tenen, l'MVT. M'agradaria saber, doncs, això, si vostè creu, doncs, que la seva eina és suficient i té la suficient garantia per afirmar-ho, no?, perquè hi ha hagut infecció i que aquesta ha estat pel sistema Pegasus i que hi ha estat.

Vostè també ara a la seva compareixença diu que ha estat validat per Amnistia Internacional, però que li va fer una selecció de terminals. M'agradaria saber per què una selecció i per què no tots.

I després també el que he trobat, que aquest, jo crec, és el quid de la qüestió o com a mínim la qüestió que a mi més em preocupa del seu informe, a la compareixença, a les... –volia dir a la diapositiva, bé, a la presentació; sempre dic «diapositiva», se'm nota l'edat– a la presentació, vostè parla que el CNI té llicències, però vostè, en canvi, està parlant del Govern espanyol i a mi m'agradaria saber si és que ho fa de manera genèrica, Govern vol dir tot l'entramat de l'Estat, o si té alguna prova que hagi estat el Govern formalment, el que s'entén jurídicament i legalment com a govern, el que ha fet aquest espionatge? *(Veus de fons.)* Poden riure, però jo crec que és important. El senyor compareixent ha dit «govern», per tant, no sé si té alguna prova que sigui el Govern espanyol o parla de l'Estat espanyol en general o del CNI, etcètera.

Llavors a mi també, i ja acabo, president... Com li dic jo no soc tècnic, però a mi..., entenc que en el mercat hi ha d'altres companyies; tant el senyor Navarro com vostè diuen que el programari Pegasus no deixa un rastre físic de programari, o això m'ha semblat entendre, sinó que es fa en funció del tràfic de dades que hi ha a d'altres..., o a webs. Per tant, també m'agradaria saber si no hi ha la possibilitat de que això es pugui replicar per part d'altres companyies que no siguin Pegasus.

També vostè parlava de la qüestió zero clic, jo l'hi havia preguntat al senyor Navarro, també l'hi pregunto a vostè. A mi em consta –com em consta del que he llegit, no és que tingui constància física que ho hagi fet jo– que hi ha altres companyies que també fan aquest tipus d'eines, no?, amb zero clic, no és la paraula, però bé, que també fan aquesta tecnologia del zero clic. I, per tant, si han previst la possibilitat o han estudiat la possibilitat de que hi hagi altres companyies que ho estiguin fent en aquestes qüestions, en aquesta metodologia o en aquests terminals infectats.

I com que tinc moltes més preguntes, també si li sembla, i després podrà contestar o no, li faré arribar per escrit i, en tot cas, em podria contestar a aquestes.

Moltes gràcies.

El president

Moltes gràcies, senyor Aparicio. Senyor Orobitg, sí?

Jordi Orobitg i Solé

Sí; moltes gràcies, senyor president. Gràcies al senyor Campo per les seves explicacions. Bé, tots som conscients que aquí el que es tracta és que hi han unes certes divergències entre les formacions polítiques a l'hora de determinar no tant que ha existit l'atac, sinó potser la responsabilitat, perquè des del moment en què el propi Govern espanyol reconeix que té l'eina tecnològica i que l'ha utilitzat prèvia autorització, en aquest cas presumpta autorització judicial, en divuit casos dels seixanta-cinc que s'especula o s'ha determinat que existeixen, jo crec que ja la capacitat i la possibilitat és evident que és inqüestionable.

Una altra cosa, com ara qüestionava en aquest cas el portaveu del Partit dels Socialistes, és si ha existit sota el mandat d'un govern o algú dins de l'estructura governamental ha operat pel seu propi compte i sense una directriu política, cosa que seria encara més preocupant, no?

Dit això, clar, ens estem focalitzant en el «Catalangate», però en aquest cas Citizen Lab no només pel que vostè ha explicitat, sinó perquè és de domini públic, ha intervingut o ha detectat aquest tipus de *spyware* maliciós, no només amb relació a persones amb nacionalitat espanyola, sinó d'arreu del món. I jo voldria saber si és que la praxi, en aquest cas de l'organització, a l'hora de determinar aquestes infeccions, ha estat diferent pel que respecta a les víctimes a l'Estat espanyol, a les víctimes de qualsevol altre estat. I, per tant, si ha existit una..., abans se'ns deia que l'estructura de Pegasus semblava haver-se construït *ad hoc* i que s'havia radicat en territori espanyol com a repositori de totes les dades que es venien extraient d'aquests terminals mòbils. El que voldria saber és si vostès han actuat d'una forma diferent pel que respecta al «Catalangate» en altres supòsits. I, per tant, que ens ho explicités.

També ho ha comentat abans el meu company: més enllà del mateix informe de Citizen Lab i d'aquest aval que ha rebut, com vostè ha dit, amb uns casos determinats per part d'Amnistia Internacional, hi han altres tècnics que discrepen del resultat de Citizen Lab i, en aquest cas, doncs, divergeixen de les seves conclusions. Abans s'ha fet esment del senyor Gregorio Martín Quetglas i també s'ha parlat, en aquest cas, del senyor Jonatan Scott, i hem escoltat una veu per nosaltres molt autoritzada perquè és un pèrit, en el sentit de que no veia en aquestes crítiques, doncs, una raó científica i que, per tant, a ell no li resultaven útils a l'hora de desacreditar l'informe de Citizen Lab, però, home, crec que seria important també conèixer la seva opinió, ja que se l'interpel·la en aquest cas com a persona vinculada a l'organització Citizen Lab, de qui és aquest informe que ens interessa.

La problemàtica dels falsos positius també és..., crec que és important determinar-ho, no? Evidentment, qui vol qüestionar la versemblança d'aquest informe, doncs, s'agafa al que calgui i, en aquest cas, doncs, el propi reconeixement per part de la organització que en un dels supòsits o en algun dels supòsits que s'ha analitzat, ha existit un fals positiu pretén fer categoria de l'excepció. I, per tant, nosaltres el que voldríem és això, no?, determinar fins a quin punt aquest fals positiu es pot atribuir de forma indiscriminada a tota la tasca d'investigació, que és molt voluminosa per part de la seva organització.

I per la resta, home, en aquest cas entenem que una part important de les qüestions que se li han plantejat té a veure amb circumstàncies personals, que són crítiques *ad hominem*, més que a la tasca que vostè hagi pogut realitzar o l'organització amb la que ha estat col·laborant i en funció de que entenem que no són rellevants,

home, per nosaltres és que fins i tot alguna d'elles jo crec que surt ja no només de l'objecte de la pròpia comissió, sinó que en un altre àmbit podrien ser considerades gairebé delictives, algunes d'elles han sonat a amenaça. I, per tant, pel que a nosaltres respecta, nosaltres demanaríem que es focalitzés en les seves respostes a lo que és explícitament l'objecte de la comissió i tot allò que té a veure amb l'informe Citizen Lab.

Moltes gràcies.

El president

Moltes gràcies, senyor Orobitg. Senyor Rius, endavant.

Josep Rius i Alcaraz

Moltes gràcies, president. En primer lloc, moltes gràcies per comparèixer avui i donar-nos tot aquest detall i explicacions que ha fet. Jo tinc unes quantes preguntes, algunes d'elles també les he formulat al senyor Navarro prèviament en la compareixença que ha fet, i alguna pot coincidir, per tant, demano disculpes.

Però m'interessaria saber Citizen Lab, d'alguna manera, quina experiència té investigant aquests casos i si a banda de Catalunya ha fet investigacions en altres països; no cal que em doni el detall si no es pot donar. La següent és, per la seva experiència, qui acostuma o qui pot adquirir aquest tipus de programari? El senyor Navarro ha fet referència a que l'estat d'Israel el considera una arma i que, per tant, requereix autorització del mateix estat d'Israel.

En tercer lloc, si sap si les dades romanen a l'Estat espanyol o poden ser traspassades a un altre estat o han de passar necessàriament també per Israel, amb tota la connotació que això pot tenir de que es puguin passar dades personals, confidencials, professionals, d'un estat a un altre per part d'un organisme estatal.

En següent lloc, la capacitat que té aquest tipus de *spyware*, de Pegasus i de Candiru, si poden monitorar totes les dades, poden arribar a modificar arxius. I, per últim, unes quantes preguntes més, perdoni. Si actualment hi ha més casos d'investigació també a Catalunya; si és que es pot respondre aquesta pregunta.

Quantes persones han intervingut en l'informe de Citizen Lab relacionat amb el «Catalangate»? Com que s'ha posat en dubte si ha pogut afectar la seva condició de català o de víctima a l'hora de dur a terme o de participar en la confecció d'aquest informe, també m'agradaria saber si ha rebut algun tipus d'amenaça o de demanda o de repressió d'algun tipus arran de la seva participació en l'informe de Citizen Lab.

Crec que amb la seva intervenció ha quedat acreditat que Citizen Lab acredita científicament infeccions en el cas del «Catalangate», però perquè no quedi cap dubte, diguem-ne, respecte a aquestes seixanta-cinc que s'han acreditat.

I, per últim, un parell de qüestions. La primera d'elles és que s'ha qüestionat una afirmació que ha fet vostè respecte a si hi havia una autoritat espanyola o el Govern espanyol. Però vaja, no em puc estar de dir-ho, des del mateix moment que el CNI ha admès que ha utilitzat Pegasus, jo crec que el CNI diria que és Govern, no?, diria que penja del Ministeri de Defensa, vaja. Llavors, només per deixar-ne constància, vull dir que d'allò i que, per tant, fins i tot les actuacions que duu a terme el CNI hi participa el mateix Govern, diguem-ne, amb una planificació anual. Aquest és el sistema de funcionament que, que jo sàpiga, té aquesta organització.

Una següent consideració i és també, bé, aquest marc de seixanta-cinc persones que s'han pogut d'alguna manera acreditar fins ara per Citizen Lab que van estar infectades o que van patir intents d'infecció, perquè se'ls va trametre SMS, doncs, configuren una amalgama i es pot fer, en aquest cas, també una traçabilitat absoluta, que tenen un denominador comú, d'alguna manera, i és que participen en un grup objectivament identificable, en els termes que el Tribunal de Justícia de la Unió Europea va manifestar recentment, perquè participen d'alguna manera o altra, o són familiars, o són advocats d'alguna d'aquestes persones en un projecte democràtic amb el qual es poden presentar a les eleccions i que per aquesta raó, doncs,

són espiades i el mateix senyor Zoido a Madrid, l'altre dia, en una entrevista, va dir que per descomptat ell justificava l'ús de Pegasus si s'havia d'investigar independentistes.

I una última consideració. L'actuació, en aquest cas de l'Estat espanyol, de les autoritats espanyoles, és de manual d'algú que vol amagar la veritat, d'algú que vol posar una actitud totalment obstruccionista per mirar d'impedir que es pugui..., de totes passades que es pugui investigar i depurar responsabilitats, probablement perquè s'haurien d'investigar a ells mateixos i s'haurien de autoimposar responsabilitats a ells mateixos o dir-li a la justícia que d'alguna manera els condemnessin.

En qualsevol cas, el compromís d'aquest Grup Parlamentari de Junts per Catalunya de que anirem fins al final per esclarir aquests fets i que els seus autors siguin castigats.

Moltes gràcies.

El president

Moltes gràcies, senyor Rius. Senyora Vinyets, té la paraula.

Montserrat Vinyets Pagès

Gràcies, president. Bon dia, senyor Campos, i, en primer lloc, moltes gràcies per comparèixer en aquesta comissió d'investigació. Li vull donar les gràcies, sobretot, per aguantar amb estoïcisme els comentaris que sobretot han vingut de part del grup polític de Ciutadans. Vull fer-li avinent que a l'últim Ple aquest grup va manifestar públicament que «*poco se les ha espiado*», una posició que ja en termes d'un partit liberal sembla difícil de sostenir avui en dia.

Miri, jo li volia preguntar, des d'aquesta perspectiva de defensa dels drets humans que té aquest institut de Citizen Lab, més enllà de l'afectació directa que hi ha indicis que ha tingut sobre la vida de persones –per exemple, vull recordar el cas de Cecilio Pineda, un periodista que va ser assassinat a Mèxic el 2017 i que es va documentar que hi havia indicis d'haver sigut espiat amb Pegasus; vostè, en la seva intervenció, ens feia referència que precisament a l'estat de Mèxic, a partir de 2015, ja es documenten casos–, més enllà d'afectacions directes a la intimitat concreta de les persones, inclús que han afectat a la seva vida, vostè considera, des d'una perspectiva global, que la utilització massiva d'aquests sistemes, d'aquest *spyware* maliciós, és un risc seriós per a la democràcia dels estats a nivell global? Aquesta pregunta a nivell general.

En segon lloc, li volia preguntar: si vostè formés part d'aquesta comissió d'investigació, en la mesura que nosaltres tenim tota una sèrie de potestats de recopilar informació, bé, unes potestats que les organitzacions de la societat civil no tenen, si vostè formés part d'aquesta comissió d'investigació, on posaria el focus o quines diligències faria? Tampoc no li demano que contesti ara aquesta pregunta, però el convido a que si vostè considera que, per part d'aquesta comissió d'investigació, ja que tindrem molts impediments per arribar a esclarir la qüestió per part de l'Estat espanyol, si vostè té alguna proposta de vies en les que insistir, doncs, jo li agrairia que les traslladés a aquesta comissió, que estem oberts a atendre les seves recomanacions.

Li volia preguntar també sobre la diferència entre Pegasus i Candiru. Entén que, per les explicacions que s'han fet, deuen ser sistemes similars, però com que s'han diferenciat, m'agradaria que m'expliqués la diferència.

També m'agradaria que m'expliqués si vostès han fet –aquesta arma, no?, que té aquesta consideració per part de les autoritats israelianes– algun tipus de gestió des de Citizen Lab, contactes amb les autoritats israelianes als efectes d'aclarir quin abast havien tingut les seves autoritzacions o no hi ha hagut aquestes gestions.

I si en algun moment vostès han vist algun contracte model que s'utilitza per part d'aquesta empresa, NSO Group, amb els diferents estats; si han accedit a alguna proposta de contracte? També si NSO Group sempre actua com a tal o bé ho fa

a través de diferents empreses interposades. És a dir que agafi la forma jurídica d'altres societats amb altres noms.

I llavors també altres preguntes que ja he fet als anteriors compareixents i que per les dificultats precisament d'investigació que presenta tot això, doncs, també les hi vull formular a vostè. Sobre el global, l'import, què val utilitzar aquest programari espia? Si això va per..., tens una llicència global que això et dona dret a infectar tota la gent que tu vulguis o s'ha de pagar per infestació; qui fa el monitoratge, si el monitoratge el fa NSO des de les seves instal·lacions o bé el fa l'estat o el comprador del programa; si es fan cursos de formació als qui adquireixen el programa, i si és difícil la seva utilització.

I, exacte, i l'última, si en l'àmbit espanyol a vostè li consta que hi hagi empreses que es dediquin a fer infestacions, a buscar dies zero que tinguin com a objecte social. Si això ara mateix és..., entenc que és una espècie d'espai que correspon a la criminalitat, però m'agradaria saber si, a banda d'Israel, on sembla que això està més a l'ordre del dia, si a l'Estat espanyol hi ha empreses que es dediquen de forma il·lícita, irregular, o potser lícita, no ho sé, que a veure si ens ho pot aclarir vostè, precisament a buscar constantment dies zero per utilitzar aquesta informació amb finalitats il·lícites.

Gràcies.

El president

Moltes gràcies, senyora Vinyets. Ara, senyor Campo, si vol contestar. Si vol dos minuts per ordenar-se, perquè veig que són molts apunts, moltes preguntes.

Elies Campo

Sí, hi ha moltes preguntes. Intentaré respondre més o menys el que m'he apuntat i si no, doncs, a la propera o m'ho envieu per correu o ho podem mirar de contestar.

Vaig una mica en format invers de les que he rebut per anar més ràpid i si no, si hi ha alguna altra oportunitat, les anem refinant. L'última pregunta ha estat del dia zero. No conec companyies que es dediquin a fer aquesta cerca en termes de maliciosa, de vendre, però és conegut que hi ha un mercat negre on companyies paguen per aquestes vulnerabilitats. Companyies com NSO tenen equips que busquen aquestes vulnerabilitats o les compren al que es diu *hackers* o desenvolupadors que troben aquestes vulnerabilitats i no les comuniquen a les empreses.

Per això, companyies com Apple o Google tenen el que es diu *bounties*, que premien desenvolupadors en lloc de vendre aquestes vulnerabilitats, les comuniquen a les companyies perquè les puguin reparar. També hi ha altres companyies que es dediquen al contrari, que es dediquen a incentivar que es trobin aquest tipus de vulnerabilitats i es comuniquin. I un exemple aquesta companyia és HackerOne, que és una comunitat de desenvolupadors que publiquen el que troben i s'informa les companyies perquè ho puguin reparar.

Què val monitoratge? En general, com qualsevol *software* i especialment en els *softwares* de seguretat, hi ha dos maneres de vendre o distribuir el *software*. Una és el que es diu *software as a service*, que vol dir que la companyia..., tu contractes la companyia i en el fons l'operes a través d'internet, però en els servidors, a la infraestructura de la companyia; i hi ha el que es diu *on premise*, que vol dir que la companyia t'instal·la la seva màquina o el seu servidor en la teva infraestructura.

Segurament en la indústria de seguretat hi ha una tendència que és que les empreses o els governs demanin que es pugui instal·lar *on premise*, perquè puguin controlar tot l'ecosistema. En el cas d'NSO segurament deu oferir les dos versions, com és comú amb aquest tipus de companyies.

En temes de preus, no ho sabem. Alguns periodistes han aconseguit trobar alguns preus, però no coneixem aquesta informació. Tenim la mateixa informació que s'ha publicat per investigacions periodístiques.

La diferència amb Pegasus i Candiru. És un *software* molt similar. En el fons és un *software* perquè s'instal·la en un dispositiu, en el cas de Candiru també cobreix dispositius d'ordinadors. Però en el fons també hi han moltes altres companyies que ofereixen *software* similar. Per tant, no és només que existeix Pegasus i Candiru, sinó que hi ha un ventall molt ampli de companyies i cada companyia té un ventall de funcionalitats diferent. Ara mateix, el focus està en Pegasus i Candiru, segurament hi han altres companyies que no estan al focus o que no es coneixen, que es deuen estar utilitzant més que Pegasus i Candiru en aquest moment.

El tema de la crisi de la democràcia, nosaltres creiem que aquest tipus de *software* té un cas d'ús que és necessari, però en general, com és el cas del «Catalangate» o altres *reports* que hem publicat, nosaltres el que fem és documentar que hi ha hagut una crisi de democràcia. No ens posem a analitzar la situació legal, política del país, però el que podem certificar és el que ha passat i certifiquem que és una crisi democràtica l'abús d'aquest tipus de *software* en societat civil.

I passo a les preguntes... Qui pot adquirir aquest programari? En general, pel que sabem, en el cas d'NSO, per exemple, ells publiquen, a la seva publicitat que fan i a la seva documentació, que només venen aquest *software* a estats o agències d'intel·ligència o de seguretat. Aquest és el cas d'NSO, però pot ser perquè hi hagin altres companyies que tinguin altres interessos o que puguin tenir un ventall més gran de venda.

On són les nostres dades? Això és una de les preguntes que també fem en les conclusions i és una de les coses que esperem que es pugui resoldre. En el cas que sigui *on premise*, segurament el que he mencionat que el *software* estigui en la infraestructura de qui hagi comprat el *software*, doncs, les dades segurament estaran allà. En cas de que sigui un *software as a service*, doncs, segurament les dades estaran en la infraestructura de l'empresa.

Les capacitats de Candiru són similars a les de Pegasus. Segons alguna documentació que s'ha filtrat sobre com funciona el *software*, es pot intuir que Candiru també permet la incorporació o la modificació de dades en els dispositius que s'infecten. Noves investigacions: no podem comunicar re conforme a víctimes que no ens hagin donat el consentiment per fer-ho públic.

Hem fet investigacions al llarg de tot l'abast mundial d'altres països i són conegudes i estan a la nostra pàgina web, per si tenen interès en trobar-les.

Ha afectat que jo sigui català o sigui afectat o víctima? No. I això és una pregunta que ja vam rebre per part d'alguns membres del Parlament Europeu i es va respondre també i es va fer pública la carta, això està a la web de Citizen Lab. I és comú, en aquesta resposta explicàvem que és comú que casos d'abús d'aquest tipus es descobreixin perquè hi ha una víctima local que demostra que hi ha aquest tipus o que mostra els primers indicis que hi ha aquest tipus d'abusos. Per tant, a l'equip tenim moltes persones que han sigut víctimes i que treballen i contribueixen al laboratori.

He rebut amb amenaces? Una de les coses, un dels fenòmens que hem documentat d'aquest cas és la generació de desinformació constant per desacreditar el laboratori o els seus autors. També hem vist un concepte que si el cerquen d'abús online, es diu *sealioning*, que és una pràctica que hem documentat també que està passant en aquest cas. També és el cas més gran quant aquest tipus de desinformació i l'abast i la durada d'aquest tipus de desinformació que es va generant gairebé diàriament.

La pregunta sobre si aquesta investigació ha estat diferent a altres: no, hem actualitzat la mateixa manera de fer aquesta investigació que en altres casos. Ja he contestat la part del tipus de *software*, si pot ser en infraestructura del client o a través de *software as a service.*

El tema del Jonathan Scott, crec que globalment la comunitat d'Infosek no el considera com una autoritat en aquests temes i, per tant, no considerem que haguem rebut cap qüestió dels cent cinquanta *reports* que hem publicat fins ara.

De falsos positius, això ho ha explicat també José Navarro, en el sentit de que tu et pots introduir un missatge amb un *link*. Aquest *link*, si el passes per l'eina MVT, et sortirà com a positiu, però si es fa una investigació més profunda d'aquest dispositiu, hi ha moltes maneres de determinar si aquell SMS o aquell indicador és un fals positiu o no. Sí que podem dir que tots els positius que hi ha al «Catalangate» han estat verificats per l'equip, revisats, doble revisats i, per tant, és altament improbable que hi hagi falsos positius.

El tema del Govern espanyol o Estat espanyol. Aquí se m'escapen els detalls jurídics i, per tant, el que hem comunicat al *report* és que alguna agència d'intel·ligència o entitat dins de l'Estat, del Govern, i també recalcar que el CNI ha reconegut públicament que té i utilitza el Pegasus.

El tema de poder replicar, que altres *softwares* repliquin la funcionalitat de Pegasus: com ja he dit abans, n'hi han molts, molts diferents tipus de *software* que tenen funcionaments diferents, però els processos que fan funcionar aquests *softwares* són com signatures que es reconeixen d'un tipus de *software* particular. Per tant, altres *softwares* que tinguin funcionalitats similars tindran altres tipus de signatures o empremtes, com si diguéssim, que puguem identificar i atribuir a un tipus de *software*.

Per tant, funcionalitats sí; que un altre es pugui comportar com a Pegasus és difícil, perquè les signatures que es troben són particularment identificables al *software* que atribuïm.

Que hi hagin altres *softwares* que s'estiguin utilitzant i no haguem trobat? Pot ser. Ara mateix hem trobat aquest *software*. Pot ser que hi hagi algun *software* que s'estigui utilitzant que no el coneixem o no el sabem trobar. Normalment totes aquestes investigacions o aquests equips anem per darrere del que realment s'està utilitzant en aquest moment i fem les troballes més endavant. Per exemple, NSO es va fundar el 2010 i les primeres identificacions que es van fer globalment van ser el 2016, quan es va fer públic que existia aquest *software*.

Les modificacions a l'informe. Hem fet modificacions que estan recollides i estan especificades. Normalment són coses de tipus errors ortogràfics o errors de transcripció de les dates de format americà a format europeu. Totes estan documentades i publicades a la web. La versió del PDF que us he enviat és l'última versió que està penjada també a la pàgina web. *(Pausa.)*

Ah, per què no surten positius, dates en alguns i en alguns altres no? Utilitzem diferents mètodes d'anàlisi. Alguns permeten trobar més informació i alguns no. En aquells casos on hem pogut documentar les dates, ho fem públic; en els casos on la nostra metodologia o que vam poder utilitzar en aquell moment no vam trobar les dates. Això no vol dir que, amb una anàlisi posterior, amb una altra metodologia es pugui arribar a trobar més informació.

Les cinc persones que no hi ha nom..., és la decisió que van prendre aquestes persones en el procediment d'investigació i de donar el consentiment. Cada persona pot donar consentiment si vol participar a l'estudi o si vol donar el seu consentiment per fer públic el seu cas. En aquest cas, aquestes cinc persones van triar de no fer públic el seu nom o el seu rol. En el tema de l'última correcció que vam fer d'AC és un d'aquests casos. De moment, encara no tenim el consentiment per fer públic aquest cas.

L'univers és una dada que ens pregunten molt i crec que pot ser una de les dades que l'equip pugui avaluar i comunicar, si es troba adient o és important.

El tema del comentari dels cinquanta mil dispositius que va fer la membre del Parlament Europeu Sophie in 't Veld, segurament es feia referència a l'estudi de *Forbidden Stories*, que es va mencionar que havien trobat una llista de cinquanta

mil números de telèfons. No es referia a que són cinquanta mil dispositius que s'hagin analitzat. D'aquells cinquanta mil números que sortien en una llista atribuïda a NSO, Citizen Lab sí que en va fer una selecció i vam poder fer una anàlisi, però no vol dir que haguem verificat cinquanta mil dispositius. Crec que és una interpretació diferent d'aquests estudis.

La selecció amb Amnistia Internacional. Normalment fem una selecció d'una secció, d'una part de la investigació. Normalment els casos que hem comunicat són més petits i normalment són la majoria dels casos. En aquest cas, van ser una part principalment, per facilitat, i després també són les pròpies víctimes qui faciliten aquestes dades directament a Amnistia. Nosaltres no transferim aquestes dades a Amnistia perquè facin la verificació de les víctimes; els hi han d'enviar.

Quant a l'eina d'MVT, aquesta eina de pública d'Amnesty Lab, nosaltres aquesta eina no la utilitzem. Tenim la nostra pròpia eina que utilitzem i les funcionalitats de l'MVT les ha descrit també el José Navarro abans i permet revisar un dispositiu Android o iPhone i permet veure si hi han algun dels indicadors que s'han fet públic abans. Aquests indicadors són de fonts públiques tant d'Amnesty com de Citizen Lab. *(Pausa.)*

Perdoneu. Després, en qüestió de si treballem..., nosaltres no treballem per cap companyia i no rebem finançament de cap companyia, especialment si són aquelles que... No rebem finançament de companyies que poden ser subjecte de la nostra investigació.

Quant a les meves capacitats o la meva història personal, crec que no són objecte d'aquí. El que puc dir perfectament és que no soc enginyer oficial d'educació d'Espanya, però això no m'ha sigut cap problema i la majoria d'aplicacions que tenen en el seu dispositiu, els fundadors tampoc no són enginyers o no han acabat la carrera i no ha suposat cap problema perquè puguin fer aquest tipus d'aplicació. A mi professionalment no m'ha sigut cap problema per poder treballar amb companyies com WhatsApp o Telegram.

En el cas de Telegram, per exemple, la majoria de partits d'aquí, d'alguna manera, algun moment us heu posat en contacte amb mi quan treballava a Telegram i em vau demanar quan no teníem un procés de validació dels canals oficials a Telegram, si us podia ajudar a tramitar. La majoria, us vaig ajudar, inclòs el del seu partit, i em consta que la persona que jo interactuava del seu partit va acabar treballant com a assistent parlamentari del membre del Parlament Europeu del vostre partit. Per tant, aquesta informació vosaltres la teniu. Amb aquesta persona m'he comunicat via Telegram o via el meu correu professional.

Què més? El tema del Jordi Sànchez, que hi havia unes dates del 2020 o que havia dit que era negatiu i després positiu. Això crec que també és una mala interpretació de les coses que s'han publicat *online*. En temes del Jordi Sànchez, crec recordar que tenia diversos dispositius i pot ser que un primer sortís negatiu i l'altre personal o de feina sortís positiu. Per tant, és un cas en concret. Potser primer n'hi vam revisar un i després li vam revisar l'altre.

Empresa de comunicació. Algunes d'aquestes preguntes ja les hem contestat, ens les vau fer i els vam contestar per carta i és pública; us la puc reenviar a tots, si la necessiteu. No vam treballar amb cap empresa de comunicació. És normal que alguns casos que treballem, al final de la investigació treballem amb periodistes que ajuden a comunicar el que hem trobat. I en el cas és conegut que l'exclusiva la va fer *The New Yorker*, amb el Ronan Farrow, en un article que va sortir al *New Yorker Magazine*. Les revistes tipus *New Yorker Magazine* tenen no només el *reporter* que fa l'article, sinó també uns equips que es diuen *fact checkers* que es dediquen a revisar tots els rols de les persones que participen en aquest estudi. I, per tant, verifiquen la informació que es publica.

En el cas de WhatsApp, això ha sortit diversos cops, crec que ho he respost, però el WhatsApp va identificar que s'estaven utilitzant els seus servidors per instal·lar

Pegasus, però en cap moment WhatsApp o Citizen Lab han certificat que aquesta utilització o aquests objectius han resultat en infeccions. El que sí que es pot demostrat en WhatsApp, que això ho va identificar WhatsApp, és que es va utilitzar WhatsApp per intentar infectar. Si aquestes infeccions van ser positives o no, no ho sabem. Per això tampoc no ho comuniquem al *report*. Nosaltres, en tot cas, certifiquem que aquestes persones van ser un objectiu a través de Pegasus, però no necessàriament infeccions satisfactòries.

Bé, i aquí hem arribat. Si..., podem fer més per correu.

El president

Moltes gràcies, senyor Campo, i gràcies a la resta de grups. Ens hem allargat bastant més del que estava previst, però crec que era interessant que pogués donar resposta, si no a totes, a la majoria de preguntes. Faríem, si algun grup vol repreguntar, un minut, però un minut estricte per grup. I després vostè cinc minuts estrictes per acabar d'aclarir.

Vostè s'ha posat, com anteriorment el senyor Navarro, a disposició dels grups per si volen fer arribar preguntes per escrit i remetre a tots els membres de la comissió aquestes respostes. Per tant, faríem això.

Senyor Martín Blanco, que veig que finalment no ha hagut de marxar.

Ignacio Martín Blanco

Marxaré corrents, president. Sí; gràcies, senyor Campo. Bé, jo... Ha contestat *pro domo sua* algunes de les preguntes. En tot cas, a mi m'agradaria saber..., una important per a nosaltres és quan van contractar vostès l'any 20 el senyor José Navarro, que ha comparegut anteriorment, quan van contactar amb ell i exactament per què.

I una qüestió que crec que és bastant crucial, si més no en termes d'opinió pública, senyor Campo. Jo necessàriament..., com a grup de l'oposició hem de ser durs amb el que considerem que és una trama orquestrada per partits adversaris del nostre. En tot cas, amb unes visions diferents de la realitat de Catalunya i d'Espanya i, per tant, no m'ho tingui com una cosa personal. Però és evident que nosaltres hem de fer la nostra tasca.

M'agradaria que vostè contestés quina és la seva participació en la plataforma Tsunami Democràtic, quines són les seves relacions, i què justificaria una possible, una presumpta investigació a la seva persona, en aquest cas. Perquè, si no, tot plegat ens sembla una mica poc consistent.

Gràcies, president. Gràcies, senyor Campo.

El president

Gràcies, senyor Martín Blanco. Sap perfectament que aquesta és una comissió que toca uns temes. Si volen treballar en altres temes, proposin comissions d'investigació sobre altres temes i crec que seran més adequades les compareixences.

Senyor Aparicio.

Oscar Aparicio Pedrosa

A veure, el senyor Nacho Martín Blanco ja és suficientment gran i amb molta més experiència parlamentària que jo, però entenc que quan algú ve a comparèixer és normal que se li pregunti per tot, perquè quan ve a comparèixer...

El president

No, perdoni. Ve a comparèixer –perdoni que l'interrompi– a parlar de l'objecte de la comissió, però, escolti, poden formular les preguntes que vulguin.

Oscar Aparicio Pedrosa

Entenc que quan un compareix en aquí ho fa fent unes afirmacions i, per tant, s'ha de veure les implicacions que té aquesta afirmació i com arriba a elles. Per tant,

entenc que se li ha de deixar marge, si les vol contestar o no el compareixent, ja és qüestió, però nosaltres no crec que les puguem o les haguem de limitar.

Dit això, jo sí que li havia fet algunes preguntes i, òbviament, tampoc no tinc res personal en contra de vostè. Dit això, jo li havia fet unes preguntes que a mi em continuen quedant sobre la taula, perquè vostè ha dit que el senyor Jonathan Scott no té cap tipus de credibilitat, m'ha semblat que deia, més o menys, eh?, a efectes internacionals. Però, en tot cas, jo el que li demano és que refuti el que diu el senyor Jonathan Scott i el que diuen d'altres persones, és a dir, les qüestions tècniques que ells argumenten que no troben correctes al seu informe. Jo crec que és aquí on hem d'anar, no tant... Abans el senyor Navarro deia que no anem tant a buscar què diu la persona, sinó què diu l'informe. Doncs aquí és on nosaltres crec que, si de veritat volem esclarir què va passar o com ha passat..., que anés per aquí.

I la segona qüestió que també li dic és: vostès posen sobre la taula un informe; se'n pot, jo crec, qüestionar la credibilitat i, per tant, com que hi ha persones presumptament implicades que estan dient que hi ha diferents infeccions que vostès no van detectar, jo li pregunto i li torno a preguntar si això invalida, condiciona, el seu informe, la seva metodologia. I vostè ha comentat que no fa servir l'MVT. M'agradaria saber quin programa fa i qui l'ha validat, aquest programa.

Gràcies.

El president

Gràcies, senyor Aparicio. Senyor Orobitg.

Jordi Orobitg i Solé

Sí; gràcies, senyor president. Entenc que vostè dirigeix la comissió i, per tant, els termes del debat, però per nosaltres és molt clar quin és l'objecte d'aquesta comissió d'investigació i, per tant, el que nosaltres creiem que no és gaire lícit és mirar d'intimidar els compareixents preguntant-los qüestions que, encara que tinguessin transcendència o rellevància perquè hi concorren les circumstàncies o el fet, no són en cap cas rellevants per a l'objecte i el que busquen, en qualsevol cas, és atemorir les persones que venen a comparèixer, que venen a comparèixer pel seu coneixement directe.

I, per tant, aquest cas el que ens interessa d'aquesta compareixença és el coneixement que té, en aquest cas, com a membre d'una organització, Citizen Lab, que ha elaborat un informe, un més, com bé ens ha dit, amb la mateixa praxi que arreu del món. I arreu del món, jo crec que..., bé, és una pregunta que potser li faré ara: si arreu del món s'han trobat una contestació política com la que s'estan trobant a l'Estat espanyol o una hostilitat com la que s'ha mostrat. És evident, s'ha mostrat en aquesta mateixa compareixença.

Nosaltres també estem en contra, entenc, que se l'obligui a una prova diabòlica, que és refutar l'informe d'un senyor, Jonathan Scott, que ha fet un informe que no refuta tècnicament, que ha quedat acreditat per un tercer, allò que defensa Citizen Lab. Vull dir, que és una prova diabòlica, que era refutar alguna cosa amb evidències del senyor Jonathan Scott, qui ha fet l'informe original.

I ja acabo. Nosaltres..., només mostrar-li el nostre agraïment, perquè és evident que sense Citizen Lab, el Govern espanyol i el CNI no haguessin reconegut que han espiat amb Pegasus. La mera existència de la seva feina, i entenem que és allò rellevant, és lo que ha propiciat o ha provocat que el Govern espanyol hagi hagut de baixar del seu pedestal d'impunitat i haver de reconèixer explícitament que, per mediació del CNI, ha espiat ciutadans catalans d'una forma espúria, per nosaltres espúria. Només per això, ja mereix la pena aquesta compareixença i agrair la seva feina.

El president

Moltes gràcies, senyor Orobitg. Senyor Rius.

Josep Rius i Alcaraz

Sí; molt breument, només també, de la mateixa manera que ho hem fet en la primera compareixença, agrair-li que avui ens hagi dedicat aquest temps, que ens hagi ajudat a posar una miqueta més de llum en tota aquesta foscor que hi ha respecte a aquest cas.

I també per fer-li un agraïment a la feina que duen a terme, perquè la consolidació de la democràcia al llarg de la història s'ha fet gràcies també a molts Citizen Labs que hi ha hagut al llarg de la història. I, per tant, des d'aquí que en quedi constància.

El president

Moltes gràcies, senyor Rius. Senyora Vinyets.

Montserrat Vinyets Pagès

Sí; gràcies. Sumar-nos als agraïments al compareixent per totes les explicacions que ha donat a la comissió.

I arran d'aquesta última afirmació que s'ha fet per part del representant del Grup de Ciudadanos, on s'ha dit textualment que això és «una trama orquestrada per partits d'ideologia independentista», bé, «una trama orquestrada», jo afegeixo «per partits d'ideologia independentista», li pregunto: vostè considera que, a la vista que Citizen Lab està dotat de professionals de solvència contrastada, Amnistia Internacional també té tota una sèrie de tècnics, el senyor José Navarro també té tota una sèrie de perícia, vostè considera que el moviment independentista és capaç d'orquestrar una trama que abasti autoritats israelianes, NSO Group?, si coneix que sigui possible que tingui aquesta capacitat de gestió per orquestrar tot això.

Gràcies.

El president

Moltes gràcies, senyora Vinyets. Senyor Campo, quan vostè vulgui, les respostes i aclariments que pugui fer.

Elies Campo

El tema de l'eina de l'MVT, la utilitzem les nostres metodologies i els nostres indicadors que hem trobat. Alguns d'aquests els anem fent públics quan es troba convenient, però les nostres eines no són públiques, precisament perquè si es fan públiques els creadors d'aquest *software* poden corregir aquest petit avantatge que tenim.

Després abans m'ho he deixat: si nosaltres hem investigat independentistes o no independentistes, nosaltres no preguntem quina ideologia o quin partit polític formen les víctimes que investiguem. I si algú té un indicador creïble de que pot estar infectat, acceptem qualsevol potencial víctima de la societat civil que ens contacti.

Infeccions que no es van detallar, segurament són infeccions que han utilitzat altres metodologies. Nosaltres les que hem publicat, les podem defensar de manera forense. Això no vol dir que després d'una anàlisi per una altra metodologia, se'n puguin trobar més o que en puguem trobar altres d'altres dispositius que encara no hem revisat.

La reacció del Govern. El patró de reacció quan es publiquen aquest tipus de casos d'abús perpetrats per un estat o per un govern o per agències d'intel·ligència d'un país, el patró que han seguit ha sigut comú a altres. Primer és negar-ho, després és acceptar-ho parcialment i normalment després hi ha una justificació dubtosa de per què s'ha fet aquest patró. Normalment el veiem en cada cas. En aquest cas l'hem vist. El volum de desinformació, especialment local dins del país que hem vist en aquest cas és ordre de magnitud més del que hem vist en altres casos.

La qüestió de la trama, si el moviment independentista pot crear una trama d'aquesta manera, no ho sé. No tinc suficient coneixement o *expertise* per poder avaluar si és capaç o no de fer-ho.

I crec que més o menys he respost.

El president

Doncs moltes gràcies, senyor Campo. Moltes gràcies, senyor Navarro. Moltes gràcies als membres dels grups parlamentaris d'aquesta comissió. Si no hi ha res més, aixequem, tanquem la sessió. Aixequem la sessió i ens veiem a la propera sessió.

Moltes gràcies.

La sessió s'aixeca a la una del migdia i sis minuts.