CAS PEGASUS: VULNERACIONS DELS DRETS A LA INTIMITAT, LA DEFENSA I D'ALTRES DRETS

SÍNDIC
EL DEFENSOR DE LES PERSONES

CAS PEGASUS: VULNERACIONS DELS DRETS A LA INTIMITAT, LA DEFENSA I D'ALTRES DRETS

SÍNDIC
EL DEFENSOR DE LES PERSONES

Síndic de Greuges de Catalunya

1a edició: Juny 2022

Cas Pegasus: vulneracions dels drets a la intimitat, la defensa i d'altres drets. Juny 2022

Maquetació: Síndic de Greuges

Foto de coberta: (c) Pixabay

ÍNDEX

INTRODUCCIÓ

A mitjans d'abril de 2022, la revista *The New Yorker* es feia ressò d'un informe elaborat per Citizen Lab, de la Munk School of Global Affairs & Public Policy de la Universitat de Toronto (Canadà). L'informe posava de manifest que persones de l'entorn polític i social independentista havien estat objecte d'espionatge amb programari maliciós com Pegasus i Candiru, almenys des del 2015. El diari *The Guardian* també s'havia fet ressò d'aquests informes ja l'any 2020 i Amnistia Internacional en va elaborar un informe tècnic l'any 2021.[1]

Segons aquestes publicacions, més de 60 persones entre càrrecs polítics, advocats i persones relacionades amb el moviment independentista català van ser objectiu del sistema de ciberespionatge Pegasus, instal·lat als seus terminals mòbils. Aquests resultats tècnics han sigut parcialment confirmats pel Centre Nacional d'Intel·ligència (CNI), que admet haver investigat amb aquest sistema divuit persones, amb la corresponent autorització judicial. En tretze d'aquests casos es va fer servir el sistema Pegasus.

Tot i que l'existència de Pegasus es coneix des de fa anys, hi ha alguns factors clau que augmenten sensiblement la preocupació actual: en primer lloc, Espanya és el primer cas en què un govern europeu admet l'ús d'aquest tipus de sistema i, en segon lloc, els objectius de la investigació són càrrecs polítics electes d'alt nivell, com ara l'expresident del Parlament Roger Torrent o l'actual president de la Generalitat, Pere Aragonès. A més, les noves notícies de casos a Polònia, Hongria, Alemanya i Bèlgica fan palès l'ús comú d'eines de ciberespionatge dins de la Unió Europea. L'últim gir de la història ha estat el descobriment que alts càrrecs del govern espanyol també han estat espiats amb el mateix sistema Pegasus (Pedro Sánchez, com a president, i Margarita Robles, com a ministra de defensa).

El Síndic de Greuges de Catalunya té la funció de protegir i salvaguardar els drets fonamentals dels ciutadans de Catalunya quan aquests drets estan en perill per accions de l'Administració pública. L'informe del Citizen Lab palesa un espionatge massiu a ciutadans catalans vinculats a tesis independentistes o a persones relacionades amb aquests ciutadans, i a la seva defensa jurídica. Evidencia igualment que aquest seguiment s'ha dut a terme mitjançat la instal·lació clandestina als seus telèfons mòbils d'un programa ocult elaborat per l'empresa israeliana NSO Group.

Arran d'aquests esdeveniments, es van posar en marxa determinats mecanismes institucionals, el 4 de maig de 2022, es va constituir la Comissió de Secrets Oficials del Congrés de Diputats (després de tres anys de legislatura) i hi va comparèixer qui aleshores era la directora del CNI. De la seva compareixença es va poder concloure que divuit personalitats catalanes, sempre vinculades a plantejaments independentistes i en bona mesura sense cap diligència penal oberta en contra seva, van ser monitoritzades pel CNI, molt singularment entre el desembre de 2019 i el primer semestre de 2020. Segons va relatar la ja exdirectora del CNI, tots els seguiments tenien autorització judicial i seguien la Directiva d'intel·ligència que va emetre el govern espanyol el 2019.

Cal recordar que aquesta directiva és secreta, com ho són les activitats del CNI –incloses les peticions al magistrat del Tribunal Suprem que ha d'autoritzar les intervencions que afecten drets fonamentals dels ciutadans que es vol investigar– i com ho són, també, les seves resolucions. Pel que fa a les sessions de la Comissió de Secrets Oficials del Congrés de Diputats, també són secretes.

El maig de 2020 el Síndic de Greuges va obrir una primera actuació d'ofici sobre el presumpte espionatge de l'aleshores president del Parlament Roger Torrent. El document es va adreçar a l'Agència de Ciberseguretat de Catalunya, que va informar que les seves investigacions respecte al possible compromís dels terminals pel programari maliciós Pegasus no eren concloents.

[1] A banda de l'informe, és convenient consultar-ne també l'apèndix D i l'apèndix E.

Tanmateix, el 19 d'abril de 2022, davant les noves informacions publicades i l'abast que van tenir, el Síndic va obrir una nova actuació que va traslladar al Defensor del Poble, com a institució constitucional encarregada de vetllar pels drets davant de totes les administracions de l'Estat, inclòs, per tant, el CNI. El Defensor del Poble, que ha tingut accés a totes les autoritzacions judicials relatives a l'espionatge de les divuit persones esmentades més amunt, ha conclòs la seva investigació amb una resolució amb data de 18 de maig de 2022. També és interessant fer esment al recent informe d'Amnistia Internacional *Pegasus: denuncias de vigilancia masiva en España*.

A partir de l'informe de Citizen Lab, de les referències que n'han fet els mitjans de comunicació, de les intervencions parlamentàries i de les compareixences d'alts càrrecs públics del govern central i de l'informe del Defensor del Poble, el Síndic es troba en disposició de presentar un breu informe institucional pel que fa a l'abast de l'impacte sobre els drets fonamentals d'una intervenció com la que permet programari maliciós com Pegasus i Candiru. L'informe està dividit en dues parts: la primera, de caràcter tècnic, exposa les característiques tecnològiques i el funcionament d'aquests programes i la segona se centra en com aquests programes poden afectar els drets fonamentals.[2]

[1] Per a la primera part, el Síndic ha comptat amb la col·laboració de l'empresa Evidentia, especialitzada en peritatge informàtic i per a la segona, del professor Joan J. Queralt, catedràtic de Dret Penal de la Universitat de Barcelona.

I. CIBERESPIONATGE: CONSIDERACIONS TECNOLÒGIQUES PER A LA CIUTADANIA

1. TIPUS DE SISTEMES DE CONTROL, MONITORITZACIÓ I ESPIONATGE

L'objectiu dels sistemes de ciberespionatge com Pegasus és l'accés a informació confidencial i íntima, i a comunicacions dutes a terme amb dispositius informàtics. D'entre tots els dispositius informàtics que existeixen en organitzacions empresarials i personals, el que més informació sensible conté és el telèfon mòbil.

Des de l'aparició dels telèfons intel·ligents, i amb l'enorme popularització dels telèfons iPhone (Apple) i dels que estan basats en Android, les persones emmagatzemem enormes quantitats d'informació personal, com ara fotografies, vídeos, documents, correus electrònics, missatgeria electrònica, historial de navegació a Internet, aplicacions, etcètera. A més, aquests dispositius integren càmeres de vídeo i micròfons, que poden ser activats o desactivats per aplicacions i pel sistema operatiu del terminal, i sistemes de geoposició basats en GPS, xarxes wifi, telefonia mòbil i fins i tot Bluetooth.

Els terminals mòbils són, sense cap dubte, el primer objecte de la història de la humanitat que ho sap gairebé tot sobre nosaltres, i sempre els portem a sobre. Per aquest motiu, la informació que contenen és molt preuada per a empreses, organitzacions i persones.

És important entendre que un control o una monitorització d'un terminal mòbil no és sempre il·legal o no consentit. Tothom està sent monitoritzat d'alguna manera en qualsevol moment. Per exemple, la xarxa de telefonia ha de saber on és el terminal mòbil en cada moment per dirigir-li les trucades i la llei obliga els operadors de telefonia a guardar i fer disponible aquesta informació per a les forces i els cossos de seguretat de l'Estat (FCSE), sempre amb la tutela judicial corresponent, a fi d'investigar casos penals de consideració greu.

Amb la mateixa motivació, la llei també obliga les empreses proveïdores de serveis digitals a guardar les dades d'accés dels seus clients i usuaris durant un any. Per això, els proveïdors de correu electrònic o de pàgines web han d'emmagatzemar informació que podria identificar les persones que utilitzen els seus serveis.

En el món laboral, està molt ben regulat l'ús de la geoposició GPS per conèixer la posició dels treballadors a l'hora de fer certes tasques, fins i tot fent servir els serveis de geoposició dels terminals mòbils corporatius. La jurisprudència actual permet que, en certes condicions, l'empresa pugui controlar les eines informàtiques, incloent-hi el correu electrònic, per garantir la política de seguretat corporativa. També hi ha hagut sentències recents que han legitimat, també en certes condicions, l'ús de programes que fan captures de pantalla dels ordinadors del personal. Ara bé, això no vol dir que tots aquests productes informàtics siguin legals a Espanya.

La gran diferència entre aquests sistemes comercials i sistemes com Pegasus és que els productes comercials normalment requereixen accés físic al terminal mòbil o a l'ordinador (o a la xarxa local que utilitzi), i cal conèixer-ne el PIN d'accés o la contrasenya administrativa. És a dir, és molt difícil que els puguin utilitzar persones que no pertanyin a un cercle molt proper a la víctima.

És molt important entendre que en condicions normals és molt difícil que un ciutadà mitjà pugui ser espiat per un veí o veïna, una persona coneguda, l'exparella, un company de feina, etcètera. A més, la gran majoria de sistemes operatius d'ordinadors i telèfons mòbils incorporen mesures per evitar que s'hi puguin instal·lar o que puguin utilitzar programes ocults per a l'usuari.

És molt complicat instal·lar i gestionar un sistema de ciberespionatge en un ordinador o telèfon remot sense autorització del propietari i de manera que el seu funcionament sigui secret (o no detectable), ja que això requereix un coneixement molt elevat de la tecnologia i recursos tècnics molt avançats. Per això, aquest tipus de sistemes, Pegasus també, només estan a l'abast de governs, agències de seguretat o intel·ligència o forces i cossos de seguretat.

La conclusió d'aquest apartat és que el ciutadà mitjà no ha de témer ser espiat per un sistema de ciberespionatge com Pegasus, i

que s'han de conèixer els diferents tipus de monitorització que es poden fer d'un terminal mòbil i com es poden produir (autoritzats i no autoritzats). El neguit que ha causat que es parli de Pegasus als diaris ha de servir perquè es faci un control de l'ús d'aquestes eines tecnològiques tan potents contra els càrrecs polítics electes i contra la ciutadania en general.

2. FUNCIONAMENT TECNOLÒGIC DELS PROGRAMES DE CIBERESPIONATGE

Tots els sistemes de monitorització, control o espionatge comparteixen una base tecnològica comuna, i la diferència rau en com s'implementa cada part. A continuació es fa una descripció de les fases comunes del cicle de vida d'una solució tecnològica de control informàtic, i es detallen les característiques de sistemes de ciberespionatge com Pegasus.

2.1. Fase de localització de l'objectiu

Aquesta fase consisteix a conèixer, per exemple, el número de telèfon de la persona objectiu del control informàtic. La dada concreta depèn del vector d'atac, i en alguns casos és important conèixer altres dades, com ara adreces de correu electrònic, tipus de terminal (inclosa la versió) o l'existència d'altres terminals propietat de la persona objectiu.

En escenaris corporatius, amb sistemes de monitorització legals, aquesta localització és trivial i no requereix cap esforç per part de la persona que vol instal·lar el programari. Ara bé, en casos de ciberespionatge, aquesta localització no seria tan trivial i podria requerir tasques i fonts d'informació només a l'abast d'agències d'intel·ligència o cossos policials. Per exemple, se sap que l'expresident de la Generalitat Carles Puigdemont va utilitzar un telèfon mòbil sense capacitats de telèfon intel·ligent, fet que va impossibilitar la instal·lació de Pegasus. S'ha publicat que l'atacant, davant d'aquesta problemàtica, va optar per infectar i controlar persones del seu entorn.

2.2. Fase d'infecció o instal·lació del programa

La naturalesa d'aquesta fase depèn en gran mesura de cada cas.

En casos corporatius, la direcció de l'empresa delega aquesta tasca en el departament d'informàtica, que té el control de tot el parc informàtic, normalment ordinadors i telèfons mòbils corporatius, de manera que la tasca d'instal·lació és trivial, ja sigui de manera presencial (la persona empleada ha de portar el dispositiu al departament d'informàtica) o remota.

És important tenir en compte que no totes les instal·lacions fetes per una empresa són legals o estan autoritzades. El caràcter legal de l'ús d'aquestes solucions en àmbit laboral no és objecte d'aquest informe, però, com a consideració general, l'empresa ha d'avisar el personal de la seva potestat de control, i ha d'emprar eines tecnològiques proporcionals als objectius que es pretenen. Els controls de geoposició o de pantalla indiscriminats i ocults se solen considerar il·legals.

És important entendre que sense un accés físic, i sense conèixer les credencials d'accés, és gairebé impossible comprometre un ordinador o un telèfon amb mitjans domèstics. A més, fabricants com Apple o Google fan un control de les aplicacions disponibles als seus mercats web (App Store i Google Play), i no permeten aplicacions de ciberespionatge.

Tanmateix, en casos de ciberespionatge i de sistemes com Pegasus, la història és molt diferent. Empreses com NSO Group provenen del món de la seguretat informàtica o del món de la ciberintel·ligència, i tenen accés a informació sobre els terminals mòbils que ni els seus fabricants coneixen.

Se sap que el sistema Pegasus utilitza forats de seguretat que no coneixen els fabricants dels terminals mòbils –i que, per tant, no estan solucionats (aquests forats es coneixen com a *vulnerabilitats de dia zero* o zero-day)– per executar programes

informàtics que fan accions que no estan permeses. És a dir, executen programes que poden esquivar les mesures de seguretat dels telèfons d'Apple o Android.

Les investigacions fetes per Citizen Lab i Amnistia Internacional revelen que NSO va fer servir diferents vulnerabilitats no conegudes de WhatsApp (sistemes Android), iMessage, FaceTime o iTunes (sistemes Apple) per executar codi informàtic no autoritzat.

Es coneixen tres mètodes d'atac: en el primer, l'atacant envia un missatge a la víctima amb la intenció de convèncer-la perquè faci clic a un enllaç. Per enganyar la víctima, s'ha trobat que es van fer servir missatges molt personalitzats, com avisos de Correus per recollir un paquet, de l'Agència Tributaria, del Registre Mercantil o fins i tot enllaços amb suposades notícies de Twitter.

Segons aquest primer mètode, quan l'usuari fa clic a l'enllaç, va a un lloc d'internet fals que fa que es descarregui un programa informàtic en el seu dispositiu i, aprofitant un problema de seguretat d'algun component del terminal, executa codi sense limitacions de seguretat.

En el segon mètode, es fa una intercepció de la navegació a Internet del terminal, ja sigui capturant el trànsit al sistema de telefonia, o mitjançant un dispositiu que emula ser una torre de telefonia (i fa que el terminal s'hi connecti). Quan la víctima entra en un lloc d'Internet no xifrat (sense protocol SSL), l'atacant injecta el codi maliciós que, com en el primer mètode, aprofita una vulnerabilitat no coneguda per tenir accés al telèfon.

El tercer mètode és el més efectiu i fa servir un problema de seguretat que es pot aprofitar sense intervenció de l'usuari. És el mètode conegut com a *zero-click*. Se sap que Pegasus, entre 2019 i 2021, podia ser instal·lat en certs telèfons Apple sense cap intervenció de l'usuari aprofitant vulnerabilitats de les aplicacions iMessage i FaceTime: l'atacant enviava una notificació al telèfon amb un contingut maliciós que permetia executar codi sense limitacions de seguretat.

Quan un telèfon és infectat d'una d'aquestes maneres, el codi maliciós descarrega i instal·la el sistema Pegasus pròpiament dit, el que es coneix com a *sistema de comandament i control* (*Command & Control* o C&C), que és un programa informàtic que, de manera oculta, espera ordres de l'atacant, com per exemple, encendre el micròfon o enviar els SMS rebuts.

2.3. Ocultació i persistència

Els sistemes de ciberespionatge com Pegasus tenen la capacitat d'ocultar-se a ulls del sistema operatiu i dels usuaris. Normalment, intenten deixar les mínimes "empremtes", per dues raons: la primera, per no ser descoberts pels usuaris i la segona, per no ser descoberts per analistes de seguretat i experts en informàtica forense.

Efectivament, quan un virus, un troià o un sistema de ciberespionatge és descobert, se succeeixen una cadena d'esdeveniments que normalment acaben amb el negoci del fabricant del sistema maliciós. Es descobreixen les vulnerabilitats que permeten la infecció inicial i la instal·lació del C&C, i normalment es comuniquen al fabricant del sistema operatiu o de l'aplicació de manera privada, per donar temps al fabricant de solucionar el problema i actualitzar tots els dispositius.

Així va passar amb Pegasus. WhatsApp va descobrir l'existència de 14.000 usuaris del seu sistema infectats per un programa maliciós que després, amb les investigacions de Citizen Lab i Amnistia Internacional, es va identificar com Pegasus. WhatsApp va solucionar el problema, el va comunicar als 14.000 usuaris i va iniciar un procés de denúncia contra NSO Group, que encara està obert al Tribunal de Districte dels Estats Units per al Districte Nord de Califòrnia en el moment en què s'ha redactat aquest informe. Això també va passar amb les vulnerabilitats d'iMessage, que es van comunicar a Apple i es van solucionar abans de publicar-se.

Normalment, la publicació i solució de la vulnerabilitat que permet la infecció acaba amb el producte de ciberespionatge. Però NSO Group ha anat trobant noves vies d'infecció (el que es coneix com a *nous vectors d'atac*). De fet, s'han documentat diverses vies d'infecció diferents entre el 2015 i el 2021.

Per als programes d'espionatge és vital la persistència, que és la capacitat del programa informàtic maliciós de continuar al dispositiu infectat després de reiniciar-lo o d'apagar-lo. Se sap que Pegasus no es guarda a la memòria no volàtil del telèfon, a fi de minimitzar la seva empremta i la seva probabilitat de detecció. Quan el sistema es reinicia, Pegasus perd la persistència i és necessària una nova infecció. Aquest inconvenient no és gaire important en terminals mòbils, ja que gairebé no s'apaguen ni es reinicien.

2.4. Enviament d'informació

Un aspecte clau dels sistemes de ciberespionatge és la comunicació amb l'atacant: l'atacant ha d'executar ordres i ha de rebre la informació de retorn del sistema infectat.

Actualment, gairebé cap producte de control remot informàtic fa connexions directes entre la persona que controla i el dispositiu controlat, sinó que es fan connexions a uns servidors centrals que en gestionen les interaccions i les gestions. D'aquesta manera és més fàcil evitar mesures de seguretat bàsiques com ara els tallafocs, perquè se solen configurar per filtrar el trànsit de dades des d'Internet a la xarxa interna, però no solen filtrar les connexions des de la xarxa interna a Internet. Moltes aplicacions legals i comunes fan servir aquesta estratègia.

Les aplicacions de control remot o monitorització senzilles o legals fan servir, normalment, una xarxa de servidors intermedis propis del fabricant del programa que són fàcilment identificables. En aquests casos, si s'investiga el trànsit de dades que genera el sistema de control, és possible identificar el tipus de programari i el seu fabricant, tot i que no es pot identificar, generalment, la persona o l'organització que està controlant el dispositiu.

En canvi, sistemes com Pegasus fan servir una estratègia més complexa. Per començar, es creu que fan servir un conjunt de servidors intermedis per a cada client de Pegasus. D'aquesta manera s'asseguren que un client no pugui comprometre la informació d'un altre al mateix servidor ni accedir-hi.

A més, s'ha comprovat que NSO Group ha posat en pràctica mesures per dificultar la identificació dels seus servidors intermedis. És a dir, l'anàlisi d'un terminal mòbil permet identificar el servidor intermedi amb el qual es comunica, però l'anàlisi d'aquest servidor intermedi no permet, directament, que s'associï amb NSO Group.

Tant Citizen Lab com Amnistia Internacional han aconseguit identificar un bon nombre de servidors de control de Pegasus a Internet. Les seves investigacions han permès identificar la "signatura" de Pegasus; és a dir, determinar un patró de comportament propi dels servidors de control de Pegasus. Una vegada determinada aquesta signatura, s'han pogut identificar altres servidors de control d'NSO.

De fet, cada vegada que Citizen Lab o Amnistia Internacional han publicat detalls de com són els servidors de control de Pegasus, NSO els ha canviat, i hi ha incorporat cada vegada més mesures per intentar ocultar-los a Internet. S'han trobat fins a quatre versions de servidors de control de Pegasus, cadascuna corresponent a una versió i una època del sistema.

Una monitorització continuada del trànsit que generen dispositius sospitosos d'haver sigut infectats amb Pegasus pot confirmar-ne la infecció, tant pel volum de dades generat (si no està justificat per les aplicacions i l'ús del sistema) com pel conjunt de servidors als quals les envia. De fet, se sap que el CNI va poder confirmar amb aquest mètode les infeccions als mòbils del president Pedro Sánchez i la ministra de Defensa Margarita Robles.

2.5. Capacitats del sistema Pegasus

Se sap poc sobre les capacitats concretes del sistema Pegasus, però s'han publicat algunes llistes de funcionalitats, que inclouen la gravació de trucades; la lectura de missatges d'SMS, iMessage i WhatsApp; la lectura de correus electrònics; l'historial de navegació; les llistes d'aplicacions instal·lades; l'activació remota del micròfon i gravació; l'activació remota de la càmera, i la retransmissió. No s'ha trobat que inclogui l'espionatge de l'aplicació de missatgeria segura Signal, que el sistema de

ciberespionatge Candiru, competència de Pegasus i que també s'ha fet servir contra polítics catalans, sí que inclou.

Se sap, també, que Pegasus es pot instal·lar en terminals iPhone i Android. Candiru també es pot utilitzar contra sistemes Microsoft Windows, de manera que s'estén el risc d'infecció als ordinadors.

Les funcionalitats més mencionades dels sistemes de ciberespionatge són passives, en el sentit que es limiten a agafar informació i dades existents al telèfon i a enviar-les a l'atacant mitjançant els servidors C&C intermedis. Però se sap que alguns d'aquests sistemes també tenen "funcionalitats actives", amb les quals l'atacant pot enviar correus electrònics i missatges suplantant la identitat de la víctima. Se suposa que l'objectiu principal d'aquestes funcionalitats és l'activació de comptes (banca en línia, per exemple), però no es descarta que també es puguin fer servir per introduir als terminals proves falses que puguin incriminar la víctima en accions o delictes que no hagi comès.

3. CONTROL DEL SISTEMA D'ESPIONATGE

Un aspecte important dels sistemes de control informàtic és la capacitat que tenen per al que s'anomena *auditoria*, que no és més que la capacitat de saber qui ha utilitzat el sistema, quan i per què.

En sistemes de control legals, com el cas del control informàtic d'equips o eines corporatives, el departament d'informàtica pot instal·lar una eina de control que pugui monitoritzar dades d'activitat del personal per alguna raó. Per exemple, es podria instal·lar una eina de monitorització de dades de geoposició (per alguna raó legal i autoritzada) i, tot i que el personal informàtic pugui tenir accés al sistema per gestionar-lo, no ha de tenir accés a les dades, ja que la geoposició és una dada de caràcter personal que, en alguns casos, pot ser molt sensible.

Els sistemes informàtics moderns permeten aquesta "separació de poders" i a la pràctica permeten a la direcció de l'empresa confiar que el departament d'informàtica no en pugui fer un mal ús, i també complir amb el seu deure d'informació en cas que algú (recursos humans, representació sindical...) pregunti com i quan s'ha fet servir l'eina, quines dades recull i qui hi ha accedit. Les eines informàtiques modernes poden recollir un registre d'activitat no modificable pel propietari del sistema, que es pot fer servir com a prova de l'ús que se n'ha fet.

Quan es parla de sistemes informàtics que poden afectar drets fonamentals, com el dret a la intimitat o el dret al secret de les comunicacions, la funcionalitat d'auditoria hauria de ser obligatòria. Només amb aquesta funcionalitat es podrien respondre preguntes com "qui ha sigut espiat", "quant de temps ha durat l'espionatge" o "quina informació ha sigut objecte de la monitorització".

Tot i que molts sistemes informàtics actuals, com el correu electrònic, guarden certa informació d'activitat, aquestes dades no estan disponibles directament per a les persones usuàries. Per exemple, tots el proveïdors de correu guarden una relació de les dades identificatives de les connexions d'Internet que han accedit als comptes de correu. Però aquestes dades no són ni públiques ni accessibles per a la persona propietària d'un compte individual (alguns proveïdors faciliten dades només dels últims dies d'activitat). Aquests proveïdors només faciliten totes les dades mitjançant un requeriment judicial, la qual cosa garanteix proporcionalitat i utilitat en l'ús d'una informació que podria ser molt sensible.

En sistemes de ciberespionatge com Pegasus, aquesta traçabilitat de l'ús del sistema hauria de ser una funcionalitat essencial, però per ara NSO Group no ha facilitat cap informació en aquest sentit de l'activitat de Pegasus en els casos que han sortit a la llum pública i, fins i tot, hi ha informacions contradictòries sobre si realment NSO pot saber com i quan els seus clients han utilitzat el seu sistema.

D'una banda, se sap que NSO Group instal·la un conjunt de servidors intermedis dedicats a cada client per raons de seguretat. Costa de creure que NSO no monitoritzi l'estat i l'ús del sistema de cada client, per exemple, per afegir més

servidors en cas que la demanda de servei d'un client augmenti.

A més, les empreses de ciberespionatge solen estar sotmeses a un control important per part dels seus governs. Se sap que NSO Group ha de rebre autorització del govern israelià per oferir els seus productes a nous clients, que es limiten a governs, agències d'intel·ligència i cossos de seguretat de països amb interessos comuns.

Aquest control governamental es produeix també amb altres empreses de ciberespionatge israelianes (Candiru, QuaDream, Paragon) i també en d'altres països, com ara Rússia (amb Positive Technologies) o la Xina (amb Computer Security Initiative Consultancy, que és una empresa de Singapur, però es creu que opera amb tecnologia xinesa).

Finalment, hi ha un acord entre Israel i els Estats Units de no fer servir aquests sistemes de ciberespionatge contra ciutadans nord-americans. Aquestes condicions s'han pogut ampliar al Regne Unit després de la publicació que càrrecs del govern d'aquest país podrien haver sigut espiats també amb Pegasus.

Aquestes consideracions fan difícil de creure que Israel no imposi a NSO Group un sistema de traçabilitat d'activitat i auditoria sobre el sistema Pegasus, de manera que es pugui saber qui l'utilitza i contra qui. També podria ser que aquestes dades siguin secretes, i que també ho sigui l'existència mateixa de les dades.

D'altra banda, les dades publicades denoten una certa manca de control per part d'NSO Group en l'ús que els seus clients fan de l'eina. S'han publicat infeccions contra dirigents polítics de països europeus com França, el Regne Unit o Espanya, en teoria aliats amb els interessos dels Estats Units (i, per tant, d'Israel). El cas espanyol és interessant, perquè ara se sap que també és client de Pegasus.

Certes publicacions podrien indicar que NSO Group facilita una eina als seus clients que, instal·lada en un telèfon mòbil, informa de si està infectat per Pegasus. Aquesta eina, però, no sembla que s'utilitzés en el cas espanyol, on la detecció sembla que ha sigut mitjançant una anàlisi de trànsit de dades.

D'altra banda, destaca l'ús de Pegasus per a una finalitat clarament diferent de les que ha anunciat NSO Group, que, en teoria, és la lluita contra el crim i contra el terrorisme. Aquesta finalitat també l'han feta pública altres fabricants d'eines de ciberespionatge i, pel que se sap, tampoc se n'ha fet cas.

Pegasus va atreure l'atenció de grups com Citizen Lab i Amnistia Internacional precisament pel seu ús contra periodistes, polítics i activistes defensors dels drets humans. Hi ha casos documentats des del 2015 a molts països diferents, com l'Aràbia Saudita, el Marroc, els Emirats Àrabs, Ruanda, França, Grècia, Polònia o Hongria.

A Espanya, crida l'atenció que el CNI hagi admès que tenia autorització per al ciberespionatge de divuit persones de l'àmbit polític català, però que en realitat s'hagin documentat més de seixanta casos d'espionatge. Encara no es coneix cap raó que expliqui aquesta diferència, i es dubta que les denúncies iniciades contra NSO Group acabin amb una explicació per part de l'empresa que pugui aclarir la situació.

En definitiva, les funcionalitats d'auditoria i traçabilitat dels sistemes de ciberespionatge, tutelades pels poders judicials, són imprescindibles per garantir un mínim control de l'ús d'aquestes eines, i aquesta capacitat de control hauria de ser transparent, amb les evidents consideracions de secret i confidencialitat que també són importants en aquests casos.

4. CAPACITAT DE DETECCIÓ I DE DENÚNCIA

Quins mitjans tècnics tenim per detectar programari de ciberespionatge als nostres dispositius? En el cas concret de Pegasus, sabem que no es guarda a la memòria interna del telèfon per minimitzar la probabilitat de detecció, però les investigacions de Citizen Lab i Amnistia Internacional demostren que, tot i els esforços d'NSO Group, la infecció i l'execució de Pegasus deixen certs indicis i

rastres que es poden considerar indicadors de compromís, i que permeten saber si un dispositiu ha sigut infectat en el passat.

En concret, Amnistia Internacional va publicar la seva metodologia d'anàlisi completa i l'ha anant actualitzant amb les dades que s'han conegut posteriorment. També ha publicat la llista dels indicadors de compromís que ha trobat per al cas Pegasus, i ha posat a disposició de qualsevol usuari d'Internet una eina gratuïta (Mobile Verification Tookit o MVT) per verificar la presència d'aquests indicadors als terminals.

La publicació de la metodologia és important, però permet, evidentment, que NSO Group tingui l'oportunitat de canviar el seu programari per evitar que Pegasus, en les noves versions, deixi aquests indicis i sigui més difícil de detectar. A més, ja han sortit també eines informàtiques que injecten aquests indicadors en mòbils, de manera que es provoquin falsos positius.

Citizen Lab només ha publicat la seva metodologia parcialment i ha fet una anàlisi de contrast (*peer-review*) de la metodologia d'Amnistia Internacional; és a dir, manté certa capacitat de fer un rastreig de possibles infeccions.

Hi ha altres mètodes de detecció. Per a empreses grans o mitjanes, l'anàlisi de les connexions fetes amb els telèfons corporatius i del volum de dades enviades pot permetre identificar la presència de sistemes de ciberespionatge no coneguts pels sistemes d'antivirus tradicionals. Per a empreses i particulars, també hi ha el recurs de contractar una empresa de peritatge informàtic o d'informàtica forense.

II. AFECTACIONS A DRETS FONAMENTALS

1. PREVISIÓ LEGAL EN MATÈRIA D'INTEL·LIGÈNCIA

El dret a la privacitat i al secret de les comunicacions està recollit en l'article 18 de la Constitució espanyola. Per la seva banda, l'article 12 de la Declaració universal dels drets humans i l'article 17 del Pacte internacional de drets civils i polítics reconeixen que ningú no pot ser objecte d'intromissions arbitràries en la seva vida privada, la seva família, el seu domicili o la seva correspondència. Finalment, l'article 8 del Conveni europeu de drets humans estableix el dret a la vida privada i familiar, sobre el qual només són acceptables ingerències de les autoritats públiques que estiguin establertes per llei, per assolir unes finalitats específiques (inclosa la seguretat pública i la integritat territorial) que siguin necessàries en una societat democràtica.

Així doncs, els drets fonamentals no són il·limitats i, en determinats supòsits i determinades condicions, poden quedar afectats, sempre respectant-ne el contingut essencial. Aquestes restriccions i els procediments per dur-les a terme han d'anar acompanyades, tal com estableix la Constitució, de normativa específica en format de llei orgànica.

Aquestes ingerències en els drets fonamentals poden tenir un caràcter individual i afectar un subjecte o un petit grup de subjectes relacionats entre si, o poden tenir un caràcter més general i afectar els subjectes habituals d'un territori. Entre les primeres, tenim les més freqüents, que són les que deriven d'una investigació penal i, si escau, de les condemnes per delictes. Les previsions des de la detenció fins a l'empresonament de persones, passant per limitacions en els drets que afectin la intimitat en les seves diverses vessants o la propietat, estan previstes en les lleis processals. L'extralimitació en la posada en pràctica d'aquestes lesions, en principi legítimes, són sancionades també per la llei, ja sigui declarant la nul·litat de les mesures adoptades o exigint responsabilitats personals a qui les hagi adoptat o executat.

En aquest sentit, les mesures que s'adopten per mandat o autorització expressa de la Constitució són bé de caràcter investigador, com les diligències penals, en què s'analitzen uns fets perquè hi ha indicis de la comissió d'un delicte o bé de caràcter defensiu o preventiu, davant de determinats perills establerts en la mateixa Constitució, com per exemple l'estat d'alarma en diverses intensitats que s'ha viscut recentment a causa de la covid o els estats d'excepció o de setge.

Hi ha un gran nombre de mesures que es poden emprar en defensa de l'Estat, enteses en sentit ampli i més enllà dels conceptes tradicionals i legals de la seguretat nacional. Davant de determinats indicis, la llei preveu que una institució concreta i específica, que depèn del Govern i segueix les seves directrius anuals, el CNI, pugui posar en marxa investigacions tant de subjectes aïllats com, més freqüentment, de grups de ciutadans, espanyols o estrangers, que puguin afectar l'ordenament constitucional vigent.

Per dur a terme aquestes funcions d'intel·ligència (és a dir, una investigació per obtenir informació i la interpretació d'aquesta informació per donar-li sentit), d'acord amb les previsions legals, pot ser necessari, d'una banda, dur a terme escorcolls en llocs tancats, com ara domicilis o despatxos, i, de l'altra, comprovar certes comunicacions. Les funcions que de manera més o menys difusa encomana la llei al CNI (Llei 11/2002, art. 4), comporten unes necessitats d'immissió en els drets que integren la intimitat personal, familiar i professional.

La cobertura constitucional d'aquestes intervencions es troba en l'enunciat genèric de l'article 18.3 de la Constitució, que les sotmet a autorització judicial: "Es garanteix el secret de les comunicacions i, especialment, de les postals, telegràfiques i telefòniques, excepte en cas de resolució judicial".

Emparada en aquesta habilitació, la Llei reguladora del control judicial previ del CNI preveu que aquest organisme sol·liciti a un magistrat del Tribunal Suprem la "intervenció de les comunicacions" (Llei orgànica 2/2002, article únic). La llei no especifica que aquesta

actuació hagi de ser motivada i, a més, pot ser reiterada sense límit. Dels resultats de les investigacions no se'n ret compte davant del magistrat que les va autoritzar, i ni tan sols la petició ni la resolució han de formular-se per escrit. Això sí, en cap cas els resultats d'aquesta mena d'investigacions es poden integrar en un procés penal, atès que responen a una mecànica diferent de la del procés penal, tant materialment com formalment, és a dir, en contingut i garanties.

2. DIFERÈNCIES ENTRE INVESTIGACIÓ PENAL I INVESTIGACIÓ D'INTEL·LIGÈNCIA

La investigació penal es posa en marxa perquè hi ha indicis raonables de la comissió d'un fet amb caràcter de delicte. Per contra, les investigacions d'intel·ligència es duen a terme per observar què passa en àmbits no fàcilment accessibles, més aviat clandestins o, com a mínim, allunyats de l'escrutini i l'observació públics, però sensibles als objectius funcionals del CNI, sense que aquests afers hagin de tenir ni tan sols indiciàriament caràcter de delicte. Per això, a diferència de les investigacions penals, les investigacions d'intel·ligència constitueixen investigacions prospectives, una modalitat prohibida constitucionalment en les investigacions penals, i són més proclius, per tant, a la invasió d'esferes d'intimitat de manera no sempre legítima.

El bé que es protegeix en una investigació penal és el que integra l'objecte de protecció de cada definició legal de delicte; és a dir, la vida, la llibertat, la integritat sexual, la intimitat... En canvi, els objectius que defineixen les activitats d'intel·ligència no estan estrictament definits a la Constitució i els que sí que es defineixen ho estan amb un grau d'indeterminació que permet un radi d'acció amplíssim, amb fàcil perill de desbordament.

En aquest punt convé comparar els requisits que han de seguir les ordres judicials que afectin drets fonamentals en un procés penal o en unes actuacions d'intel·ligència. La regulació del procés penal en matèria d'investigacions que afectin els drets que integren la intimitat dels ciutadans està estricament regulat, especialment després del 2015. Per regla general, la inobservança dels requisits legals comporta, com a mínim, la nul·litat de les proves que s'hagin pogut obtenir mitjançant aquestes ingerències defectuoses. En canvi, no s'observa cap previsió legal que permeti expulsar de l'ordenament jurídic actuacions d'intel·ligència que no complexin ni els requisits mínims que preveu la llei del sector.

Ara bé, centrats en el tema que motiva aquest informe, l'anomenat *Catalan Gate*, atès que no ha transcendit el contingut de cap petició d'autorització per part del CNI, en principi no hi ha possibilitat de valorar si la petició administrativa ha complert, encara que sigui de manera aproximada, els paràmetres que han de revestir tant les peticions policials en seu d'investigació criminal com les interlocutòries judicials que les autoritzen. Aquesta doctrina i la seva base legal podrien donar certa entitat a la simple regulació prevista per l'actuació governativa d'intel·ligència, tant pel que fa a la formulació de la petició de l'autorització judicial com a l'atorgament de l'autorització.

Val a dir, certament, que el Defensor del Poble, després d'analitzar les interlocutòries del Tribunal Suprem que autoritzaven les intervencions en els dispositius mòbils de les divuit persones objecte de supervisió en el cas Catalan Gate, ha constatat "l'elevat grau de detall en la informació de què disposava el magistrat del Tribunal Suprem per poder adoptar una decisió d'autorització o no autorització" i que les interlocutòries "estaven extensament motivades, essencialment fonamentades en fets concrets".

No obstant això, tenint en compte els drets sobre els quals versa la petició d'autorització per part dels serveis d'intel·ligència, i en vista de les informacions fetes públiques per Citizen Lab, que no ha contradit ningú, el Síndic planteja, com a mínim, una sèrie de dubtes sobre els possibles drets fonamentals afectats, i conclou amb unes recomanacions derivades de la doctrina del màxim òrgan protector dels drets fonamentals a Europa: el Tribunal Europeu de Drets Humans (TEDH).

Amb les dades de què es disposa avui, i atès el secret legal que aixopluga les actuacions practicades (tant les divuit que s'han

reconegut públicament com les altres), es pot concloure que tota ingerència en els drets fonamentals previstos per la Constitució es basteix sobre dos pilars essencials. Un és la necessitat, i l'altre, la proporcionalitat. El pressupòsit dels dos pilars és el principi de legalitat.

A continuació s'analitzen aquests elements en relació amb els drets que, presumiblement, han estat o han pogut estar afectats per les ingerències que s'han esmentat.

3. PRINCIPIS RECTORS DE LES INGERÈNCIES EN MATÈRIA DE DRETS FONAMENTALS (I): EL PRINCIPI DE LEGALITAT

Comencem per la base comuna de totes les afectacions provocades pels poders públics que volen ser justificades en l'esfera dels drets dels ciutadans. La condició o el requisit de legalitat opera en una doble vessant. La primera resulta òbvia: la mesura que s'ha de practicar en l'esfera dels drets bàsics ha de venir específicament prevista per la llei; en aquest cas, la llei ha de ser la mateixa Constitució, desenvolupada per llei orgànica. Pel que fa al que aquí interessa, la llei preveu que cal autorització judicial per accedir a les comunicacions dels subjectes que cal monitoritzar.

3.1. El principi de legalitat: àmbit de la ingerència

Tal com s'ha vist en la primera part d'aquest informe, atès que la ingerència duta a terme per la tecnologia Pegasus suposa un accés íntegre als telèfons mòbils, cal subratllar que, amb la llei a la mà, és il·legal accedir al conjunt d'informació i a les dades que incorpora el telèfon mòbil infectat. En efecte, segons la Constitució, només és lícit accedir a les comunicacions, és a dir, a contactes interpersonals mitjançant el sistema de xarxes físiques o virtuals de què es disposa. No és lícit, en canvi, accedir a la resta d'informació que pot contenir un dispositiu d'aquest tipus, que és molta.

Aquest extrem és de vital importància si tenim en compte que, com s'ha vist, els telèfons intel·ligents són molt més que telèfons convencionals; són, de fet, ordinadors miniaturitzats, multifuncionals, amb infinitat de dades que no tenen res a veure amb comunicacions interpersonals. Per exemple, l'agenda diària, els contactes, els arxius documentals, gràfics, sonors o d'imatges en qualsevol format (fins i tot pel·lícules de tota mena), les dades escanejades, els codis QR o les fotos familiars que es duen als telèfons no són comunicacions, sinó objectes que pertanyen a la persona titular del telèfon, independentment de la manera en què les fotos, les dades o altres documents s'hagin introduït a l'aparell.

És més, l'accés als documents o a d'altres tipus d'arxius que es troben al núvol i que poden ser descarregats als telèfons no constitueix pròpiament una comunicació, atès que no s'hi estableix una comunicació interpersonal. En efecte, la comunicació no es fa amb una altra persona diferent de la titular, sinó que configura l'accés en remot a un arxiu propi que es pot descarregar en la seva totalitat o en part, o fins i tot que simplement es pot visualitzar, sense contactar amb ningú més.

Igualment resulta d'interès que, a diferència del que succeeix en matèria d'investigació criminal legítimament autoritzada, el seguiment de persones mitjançant el telèfon és aliè al concepte legal de comunicació, atès que la deambulació, el trasllat o el transport d'una persona físicament no implica cap intercomunicació personal. Seguir una balisa instal·lada en un telèfon mòbil no és cap comunicació entre dos subjectes, un dels quals és objecte de la investigació.

Així, amb la legislació espanyola a la mà, i sense necessitat de verificar el contingut de cap petició ni de cap autorització judicial, resulta legítim afirmar que en cap cas es pot accedir legalment a un telèfon, en una investigació d'intel·ligència, per obtenir informació diferent de les comunicacions interpersonals.

3.2. El principi de legalitat: les raons de la ingerència

Un segon vessant de la legalitat referit al camp de la intel·ligència té relació amb els motius o les raons que afecten la integritat de l'anomenat *sistema institucional vigent*.

Certament, es tracta d'un concepte vaporós i poc definit i definible. Ara bé, no té res a veure amb la integritat del sistema institucional dirigir les actuacions d'intel·ligència a les comunicacions interpersonals quan es refereixen a situacions que afecten una pluralitat d'altres drets fonamentals diversos de la intimitat, o a objectius aliens d'aquesta institucionalitat bàsica, com poden ser interessos polítics, personals o comercials.

D'aquesta manera, les actuacions resulten òrfenes de cobertura legal i, per tant, el principi de legalitat queda vulnerat en aquest vessant quan, com hem sabut, s'observen comunicacions i més elements integrants de la intimitat de les persones i que afecten altres drets fonamentals, com és el dret de defensa o les negociacions entre partits després d'uns comicis per formar govern.

a) El dret de defensa

El dret de defensa no només integra la defensa de les pretensions de les persones interessades davant els tribunals i altres poders públics, sinó que es basa en la confidencialitat que presideix sense excepcions les relacions entre advocat i client. En el cas més extrem, el de les imputacions dels delictes més greus –en què, per tant, ja hi ha una causa processalment constituïda–, el dret a la defensa i la llibertat de les comunicacions entre el lletrat i el seu client en qualsevol lloc i sota qualsevol circumstància és inalienable.

Hi ha drets, com la llibertat personal o el secret de les comunicacions, que poden ser suspesos individualment o col·lectivament. No és el cas de la confidencialitat entre advocat i client, que, com diem, és la base del dret de defensa, fet que, al seu torn, constitueix una de les manifestacions del dret a un procés públic amb totes les garanties. Aquest dret no pot patir sota cap circumstància cap mena de restricció. Tant és així que la vulneració d'aquest dret ha comportat alguna sanció penal greu, fins i tot contra algun jutge, i ha significat la inhabilitació per exercici de funcions públiques dels responsables.

En el context de les autoritzacions judicials prospectives es pot produir una situació crítica que podria deixar de fet inoperatiu el dret a la defensa i a la confidencialitat entre advocat i client. Atès que els magistrats que poden donar aquestes autoritzacions pertanyen a dues sales en què algunes de les persones investigades tenen plets pendents –és a dir, les sales contenciosa administrativa i penal, ambdues del Tribunal Suprem–, aquests magistrats, en autoritzar l'observació de les comunicacions d'aquestes persones podrien entrar en contacte, i en secret, amb les seves estratègies processals. Això comportaria una lesió irreparable del dret de defensa.

Cal afegir, tal com s'indica més endavant, que atès que la designació d'aquests magistrats no es fa segons un sistema públic i objectiu, sinó segons un sistema adreçat a la tria d'un jutge determinat per raons que no consten en la llei, l'ombra de dubte sobre el dret de defensa encara es fa més gran i s'acosta més a la línia d'un risc constitucionalment inassumible.

b) El dret a la participació política

D'altra banda, tampoc no és susceptible d'afectació legítima, sigui quin sigui el context, el dret de participació en els afers públics. Accedir a les comunicacions i a altres contactes, interceptar documents o observar negociacions, siguin formals o mers contactes entre formacions polítiques, és radicalment contrari a la legislació vigent. La confidencialitat que presideix aquestes negociacions és la que les parts li vulguin donar i, per tant, correspon només a les forces en tràmit de negociació revelar al públic el que van acordant o l'estat general de les negociacions. Infringir aquest dret és encara més greu, atès que es vulneren els drets del representats i dels seus representants. En efecte, es tracta de negociacions entre forces polítiques sobre les quals no hi ha cap presumpció d'il·legalitat, persegueixin les finalitats que persegueixin, ja que la Constitució espanyola no és, a diferència d'altres, una constitució militant. El dret a la participació en els afers públics ha quedat, en aquest cas, compromès.

3.3. El principi de legalitat: el jutge predeterminat per la llei

El jutge designat per autoritzar les ingerències en les comunicacions dels ciutadans és designat *ad hoc*, sense concurs, pel Ple del Consell General del Poder Judicial (art. 127.4 de la Llei orgànica 6/1985, d'1 de juliol, del poder judicial).

La Constitució estableix com a dret fonamental bàsic de la persona, com a dret fonamental que garanteix la imparcialitat objectiva judicial i la seguretat jurídica, que els jutges vinguin determinats per la llei, amb caràcter general i no per a un afer concret. Amb aquesta designació personal d'un jutge per a un afer concret i tan summament delicat, es corre el risc que la competència sobre aquest afer no vingui predominada per un torn legal, com succeeix en la resta d'afers litigiosos, sinó que se cerqui un jutge per a un tipus de cas concret i únic amb unes característiques específiques. En aquest supòsit, no és la llei sinó aquestes característiques d'ordre personal el que establiria la competència. Aquesta forma de designació personal pot vulnerar el caràcter de previsió generalística d'assignació de competències, tal com preveu l'ordenament vigent per al coneixement dels afers jurisdiccionals.

La regulació actual, en alguna mesura de dubtosa constitucionalitat, sembla més aviat idònia per designar un magistrat a priori més favorable a les pretensions del CNI que a la salvaguarda dels drets dels ciutadans.

4. PRINCIPIS RECTORS DE LES INGERÈNCIES EN MATÈRIA DE DRETS FONAMENTALS (II): EL PRINCIPI DE NECESSITAT

Quant a la necessitat, és ben sabut que, tal com ha assenyalat la jurisprudència, tant ordinària com constitucional, cal que una afectació de drets fonamentals sigui realment l'últim recurs, és a dir, que no hi hagi cap altra mesura que es pugui posar en pràctica que satisfaci els objectius proposats pels investigadors. De la mateixa manera, també com apunta la jurisprudència, no es pot confondre la comoditat de l'òrgan o la facilitat en l'execució de la mesura amb la necessitat d'aquesta mesura.

La necessitat de la ingerència suposa realment l'últim mitjà de què disposa el poder públic corresponent. Dit d'una altra manera, si es disposa de maneres que, encara que siguin més dificultoses, siguin menys invasives, s'han d'emprar. Per aquest motiu, només és constitucionalment legítima l'execució d'aquestes mesures invasives de drets fonamentals en la mesura que no sigui factible una altra manera d'actuar.

Ara bé, a hores d'ara no hi ha cap element exterior i accessible que permeti valorar aquest extrem a l'hora de formular les peticions i a l'hora d'emetre la resolució judicial que les autoritzi, fins i tot condicionant-ne la pràctica al requisit de la necessitat.

A més, aquest requisit ve imposat per l'autorització de la intervenció i, si escau, per l'autorització del perllongament. Dit això cal ressaltar que no hi ha cap previsió legal respecte a la ponderació judicial del resultat final. Això té com a conseqüència que, en definitiva, la necessitat de la ingerència en les comunicacions pugui esdevenir una apreciació merament *pro forma* i mai verificada materialment per una autoritat independent.

Finalment, cal reiterar que des del punt de vista de la previsió legal només pot ser massiva l'observació de les comunicacions i no d'altres objectes que es puguin obtenir pel fet que es troben al dispositiu mòbil o en qualsevol altra mena de dispositiu que permeti comunicacions interpersonals, tant si l'abast de l'observació és sobre un subjecte com sobre un grup de subjectes.

5. PRINCIPIS RECTORS DE LES INGERÈNCIES EN MATÈRIA DE DRETS FONAMENTALS (II): EL PRINCIPI DE NECESSITAT

En aquest terreny, la proporcionalitat o, en termes negatius, la prohibició de l'excés, té un paper preponderant en el terreny de les immissions en els drets fonamentals. A l'hora d'interceptar les comunicacions dutes a terme des d'un telèfon mòbil –com els telèfons intel·ligents actuals– o des d'altres dispositius –com els ordinadors de sobretaula, ordinadors portàtils i tota mena

de tauletes que estiguin connectats a la xarxa de telecomunicacions–, no es pot accedir a altres objectes que no siguin les comunicacions mateixes. Cal recordar que en queden constitucionalment i legalment exclosos tota la resta de materials que s'hi trobin, per gran que sigui l'interès a obtenir-los i analitzar-los. Així, el mandat de proporcionalitat imposa la destrucció immediata, sense cap més contacte que aquesta destrucció, de les dades que s'obtinguin en un aparell susceptible d'observació.

Dit això, i seguint les pautes elaborades per la Comissió de Venècia de 2015[3] en relació amb les observacions d'intel·ligència i un conjunt de sentències del TEDH,[4] s'ha anat configurant una doctrina sòlida en què la necessitat i la proporcionalitat són la base de les funcions d'intel·ligència sobre les comunicacions i altres aspectes de la intimitat.

Ja no es tracta només de la concepció clàssica de la proporcionalitat com un judici sobre el fet que els beneficis de la ingerència en els drets fonamentals han de superar la inevitable lesió de drets. Es tracta, ara, a més, del fet que aquests judicis de necessitat i de proporcionalitat han de ser verificats amb posterioritat, com a mínim un cop duta a terme l'observació i valorar en quina mesura els drets a la intimitat i els altres drets fonamentals s'han vist afectats dins dels paràmetres constitucionals.

Aquesta verificació ha de tenir en compte, com a mínim, tres factors capitals. En primer lloc, la verificació del procés d'ingerència l'ha de dur a terme un ens independent, aliè a l'ens que duu a terme la investigació d'intel·ligència, el qual pot ser judicial o no. En segon terme, s'han de verificar també de manera independent els resultats obtinguts amb les ingerències en els drets fonamentals vulnerats. En darrer lloc, cal donar l'oportunitat a la persona afectada de verificar l'afectació i de poder recórrer als tribunals, arribat el cas, si observa que s'han vulnerat els seus drets constitucionals.

Cap dels organismes esmentats, ni la Comissió de Venècia ni el TEDH, no neguen la necessitat de les investigacions d'intel·ligència, fins i tot massives, en les diverses àrees més sensibles de la societat actual. Aquestes ingerències, tanmateix, s'han de dur a terme amb les garanties essencials en un societat democràtica. Al cap i la fi, el control de la legitimitat de la ingerència, que només es pot dur a terme amb posterioritat, l'han de poder fer tant un òrgan independent com la persona afectada. És el que el TEDH en les seves resolucions, denomina *end-to-end safeguards*; és a dir, poder sotmetre les ingerències en els drets fonamentals a un control del principi al final, de manera que el procés d'ingerència compleixi totes les garanties. De fet, això és el que succeeix en els procediments o en aplicacions digitals complexos, en què les verificacions dels procediments són automàtiques, sense necessitat d'afegir-hi cap element més.

El gaudi efectiu d'aquestes garanties només és possible si les persones afectades són coneixedores, en un moment donat, de la intromissió de la qual han estat objecte. Per aquest motiu, l'informe d'Amnistia Internacional de maig de 2022 no tan sols afirma que és imprescindible la supervisió judicial, sinó que les persones afectades han de ser informades, quan sigui possible, que van ser objecte de mesures de vigilància o que les seves dades han quedat compromeses.

[3] Comissió de Venècia. *Report on the Democratic Oversight of Signals Intelligence Agencies*, aprovat en la 102a sessió plenària (Venècia, 20-21 de març de 2015). Estudi núm. 719/2013, Estrasburg, 15 de desembre de 2015.

[4] Vegeu les sentències de la Gran Sala del TEDH de 4 de desembre de 2015 (cas Roman Zakharov *vs.* Rússia) i de 25 de maig de 2021 (casos Big Brother Watch *vs.* el Regne Unit i Centrum för Rättvisa *vs.* Suècia).

III. CONCLUSIONS

Els sistemes de ciberespionatge globals són una realitat a Europa i provocaran un debat i una reflexió sobre la manera en què les agències d'intel·ligència i els cossos de seguretat han de controlar l'ús d'aquests recursos tecnològics.

Els governs i les agències d'intel·ligència necessitaran de ben segur aquests serveis, ja siguin propis, com és el cas de països amb recursos tecnològics com els Estats Units, Rússia o la Xina, o contractats, com en la majoria de països europeus. També hauran d'aprendre a defensar-se i evitar situacions com les ocasionades per Pegasus a Espanya, el Regne Unit, França o Grècia.

Amb la informació de què es disposa es pot presumir que l'ús d'aquests sistemes sobre divuit ciutadans particulars ha respectat la legalitat formal, però alhora és indubtable que pot haver suposat un atemptat a drets fonamentals, inclòs el dret a la privacitat i, en alguns casos, el dret de defensa i de participació política. Per a la resta de persones presumptament espiades amb Pegasus, més de quaranta, tot fa pensar que no s'ha respectat cap mena de legalitat i que la ingerència sobre els seus drets fonamentals ha estat sense restriccions i sense cap control.

Per aquest motiu, des del punt de vista de la salvaguarda dels drets humans i les llibertats fonamentals, el Síndic de Greuges considera el següent:

1. Segons l'examen obligat per les actuacions que ha reconegut el CNI i les que han documentat Citizen Lab i Amnistia Internacional i no han estat contradites, es pot presumir que s'han produït lesions injustificades en els drets de les persones observades, en altres aspectes de la seva intimitat personal, familiar i professional, en el dret de defensa, en el dret a la confidencialitat entre client i advocat, en el dret a participar en la gestió dels afers públics per si mateixos o per mitjà dels seus representants i en el dret a jutge predeterminat per la llei. Caldria, per tant, una reparació per part dels poders públics implicats.

2. La intervenció en les "comunicacions", prevista constitucionalment i legal com a límit del dret a la intimitat, no empara en cap cas, ni tan sols amb autorització judicial, l'accés a tota la informació de què poden disposar els terminals mòbils de tipus telèfon intel·ligent.

3. Cal una reforma urgent de la Llei de secrets oficials, que s'acomodi a les regles emanades de la Comissió de Venècia i del TEDH. En aquest sentit, és necessari establir un sistema públic i col·legiat d'autorització i de control judicials respecte de les observacions de les comunicacions que en seu d'intel·ligència es demanin dins del marc de la llei. En efecte, d'una banda, cal passar d'un sistema de jutge individual a tribunal col·legiat i, de l'altra, la designació dels seus integrants ha de ser, en tot cas, pública, mitjançat el concurs corresponent entre els magistrats del Tribunal Suprem, si així s'estima. El nomenament del magistrat encarregat de les autoritzacions i dels controls no pot dependre del designi només del president del Consell General del Poder Judicial, ratificat *pro forma* pel ple del Consell.

4. Cal fixar un límit temporal a les observacions de les comunicacions, atès que amb el disseny legal actual podrien ser indefinides, sense que el subjecte observat hagués comès cap infracció de l'ordenament jurídic ni tingués coneixement que està sent monitoritzat.

5. Un cop finalitzada l'actuació governativa d'observació i conclosa amb una resolució judicial valorativa, caldria donar-ne trasllat a la persona interessada, de forma reservada, però amb accés ple a l'expedient administratiu i judicial generat, a fi que pogués al·legar el que considerés adient sobre l'eventual vulneració dels seus drets. D'aquesta manera, la persona rebria una resolució fundada jurídicament i recurrible, arribat el cas, en salvaguarda de les seves garanties constitucionals.

6. La llei ha d'expressar explícitament que queden excloses d'investigació les observacions de membres de partits polítics, sindicats i associacions de qualsevol mena que siguin legals, és a dir, constituïts conforme a les lleis i sense estar sancionats,

la qual cosa n'inclou la dissolució judicial o, fins i tot, la prohibició.

7. Ha de quedar també establerta en la lletra de la llei la prohibició d'observar les relacions entre client i advocat o d'interferir-hi de qualsevol manera. Aquestes relacions no poden ser objecte d'observació o registre en cap cas i sota cap circumstància. En aquests dos últims supòsits, la reforma de llei hauria de fer una referència especial a la responsabilitat penal si es produeixen les anomalies esmentades. Des d'aquest punt de vista, el Síndic recomana als col·legis professionals de l'advocacia de Catalunya, i al consell de col·legis en particular, que promoguin accions de garantia del dret de defensa en els casos en què les relacions entre client i lletrat s'hagin vist afectades per escoltes il·legals.

8. Els fabricants dels sistemes de ciberintel·ligència haurien d'estar sotmesos a controls d'auditoria i estar obligats a identificar clients i víctimes en certes condicions compatibles amb el secret que la seva activitat requereix. Tecnològicament parlant, aquesta capacitat de traçabilitat és possible i és compatible amb el respecte a la confidencialitat de les persones implicades. Les funcionalitats d'auditoria i traçabilitat dels sistemes de ciberespionatge, tutelades pels poders judicials, són imprescindibles per garantir un control mínim de l'ús d'aquestes eines i aquesta capacitat de control hauria de ser transparent, amb les evidents consideracions de secret i confidencialitat que també són importants en aquests casos.

SÍNDIC

EL DEFENSOR DE LES PERSONES

Síndic de Greuges de Catalunya
Passeig Lluís Companys, 7
08003 Barcelona
Tel 933 018 075 Fax 933 013 187
sindic@sindic.cat
www.sindic.cat